HETEC

V - IP

Installation and User Guide

V-IP Installation and User Guide

Copyright © 2004

Based on Firmware 04.00.01
Last updated on 24 January 2005
Document ID: p_v-ip_00en_manualv2

HETEC Datensysteme GmbH
Landsberger Straße 65
D 82210 Germering
Germany

Tel. +49 89 894367-0
Fax: +49 89 894367-99

Web: http://www.hetec.de
mail: info@hetec.de

Table of Contents

Preface ..... **vii**
- Copyright vii
- About the V-IP vii
- Limited Warranty vii
- Limitations of Liability vii
- Technical Support viii

1. The Quick Start Guide **1**
- Installation 1
- Connectors and Indicators 1
  - Front Side Connectors (Figure 1-1) 1
  - Rear Side Connectors (Figure 1-2) 2
- Connecting the V-IP to the Host System 2
- Initial Network Configuration 2
- V-IP Setup Tool 3
  - Main Window 3
  - MAC Address Detection 4
  - Authentication 4
- Configuration via Serial Interface 4
- Web Interface 5
- The Remote Console 5

2. Introduction **7**
- Introduction 7
- Features 7
- V-IP System Components 8
- When the Server is up and running 8
- When the Server is dead 8

3. Installation **11**
- Operation Overview 11
- Connectors and Jumpers 11
  - Front Side Connectors and Indicators 11
  - Rear Side Connectors 12
- Connecting the V-IP to the Host System 12
- Connecting a Local Console 13
- Connecting Ethernet 13
  - 10 Mbps Connection 13
  - 100 Mbps Connection 13

4. Configuration **15**
- Initial Configuration 15
- V-IP Setup Tool 15
  - Main Window 15
  - MAC Address Detection 16
  - Authentication 16
- Initial Configuration via DHCP Server 17
- Initial Configuration via Serial Console 17
- Web Interface 18
- Mouse, Keyboard and Video configuration 18
  - V-IP USB interface 18
  - V-IP Keyboard Settings 18
  - Remote Mouse Settings 19
  - Auto Mouse Speed and Mouse Synchronization 19
  - Host System Mouse Settings 19
  - Single and Double Mouse Mode 20
  - Recommended Mouse Settings 20
  - Video Modes 21
- Resetting the V-IP to its Factory Settings 21
  - Using the Serial Interface 21

5. Usage 23
Prerequisites 23
Login into the V-IP and logout 24
Login into the V-IP 24
Navigation 25
Logout from the V-IP 26
The Remote Console 26
General Description 27
Main Window 27
6. Menu Options 37
Remote Control 37
KVM Console 37
Telnet Console 37
Virtual Media 39
Floppy Disk 39
CD ROM 40
Creating an Image 43
User Management 45
Change Password 46
Users And Groups 46
KVM Settings 48
User Console 48
Keyboard/Mouse 51
Video 53
Device Settings 54
Network 54
Dynamic DNS 56
Security 59
Certificate 61
Serial Settings 63
Intelligent Platform Management Interface (IPMI) 65
Date And Time 66
Event Log 67
Maintenance 69
Device Information 69
Event Log 70
Update Firmware 71
Unit Reset 72
A. Frequently Asked Questions 75
B. Glossary 77
C. V-IP Video Modes 79
D. Users and Roles 81
E. Key Codes 83
F. Pin Assignment 87
VGA HD-15 87
RJ45 Connector Ethernet 87
G. Specifications 89
Sizes and Weight 89
Environment 89
Temperature 89
Humidity 89

H. V-IP Operation Advices.....91
I. HETEC Warranty Information.....93
Limited Warranty.....93
Customer Remedies.....93
No Other Warranties.....93
No Liability For Consequential Damages.....93

Preface

Copyright

Copyright 2004 HETEC Datensysteme GmbH

Landsberger Str. 65

82110 Germering

Germany This publication contains proprietary information which is protected by copyright. No part of this publication may be reproduced, transcribed, stored in a retrieval sys- tem, translated into any language or computer language, or transmitted in any form whatsoever without the prior written consent of the publisher, HETEC . HETEC acknowledges the following trademarks:

- Intel is a registered trademark of Intel Corporation.
- Windows 98, Microsoft Windows, and Windows NT are trademarks of Microsoft Corporation.
- IBM, AT, VGA, PS/2, and OS/2 are registered trademarks and XT and CGA are trademarks of International Business Machines Corporation.
- HETEC is a registered trademark of HETEC Datensysteme GmbH, Germering, Germany .

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. HETEC disclaims any proprietary interest in trademarks and trade names other than its own. Authors: HETEC Team

This document was created on 24 January 2005 .

About the V-IP

The V-IP provides server management capabilities. You can use the V-IP to manage and monitor components in your servers through a modem or LAN, even if your network is down. The V-IP offers a comprehensive hardware solution for server management.

Limited Warranty

The buyer agrees that if this product proves to be defective, HETEC is only obligated to repair or replace this product at HETEC 's discretion according to the terms and conditions of HETEC 's general trading conditions. . HETEC shall not be held liable for any loss, expenses or damage, directly, incidentally or consequentially resulting from the use of this product. Please see the Warranty Information shipped with this product for full warranty details.

Limitations of Liability

HETEC shall in no event be held liable for any loss, expenses or damages of any kind whatsoever, whether direct, indirect, incidental, or consequential (whether arising from the design or use of this product or the support materials provided with the

product). No action or proceeding against HETEC may be commenced more than two years after the delivery of the product to the buyer.

Technical Support

If you need help installing, configuring, or running the V-IP , call your HETEC OEM or VAD Technical Support representative. We invite you to access the HETEC 's Web site (http://www.hetec.de). There you shall find all modifications made after the editorial deadline.

Chapter 1. The Quick Start Guide

Installation

The V-IP redirects local keyboard, mouse and video data to a remote administration console. All data is transmitted with the TCP/IP protocol family. The V-IP can be used in a multi-administrator and multi-server environment as well. Combining the V-IP with a KVM switch allows to access multiple remote servers over one single remote console.

Connectors and Indicators

Front Side Connectors (Figure 1-1)

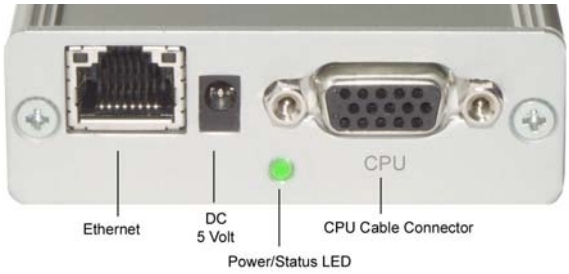

Figure 1-1. Front Side Connectors and Indicators

System port

Attach the system cable to this port.

Power/Status LED Displays the

status of the V-IP :

- LED off: the V-IP has no or not enough power
- LED blinking: the V-IP is booting up (if this process takes longer than one minute, the reason may be a lack of power).
- LED on: the V-IP is up and running.

If the V-IP is connected via USB only and the Power/Status LED tends not to stop blinking after one minute, the V-IP may not receive enough power via USB. In that case attach the enclosed power supply to the V-IP .

Power supply DC 5V Attach the enclosed power

supply to the V-IP .

- Voltage: 5V
- Current: 1.5 A

RJ45 Ethernet

UTP3/5 cables can be connected to the V-IP using this standard RJ45 jack.

Rear Side Connectors (Figure 1-2)

Figure 1-2. Rear Side Connectors

Port replicator Here you may attach an optional port replicator enabling PS/2 support, serial and local console.

Connecting the V-IP to the Host System

Perform the following steps in order to connect the KVM signals of the server system to the V-IP :

1. Connect the pre-mounted system cable to
   - The VGA outlet of your server or the local console video port of your KVM switch.
   - The USB to one of the USB interfaces of your server or your USB-KVM switch.
2. Connect the RJ45 Ethernet connector to your local Ethernet hub using a CAT5 cable.
3. Connect the external power supply to the 5V power connector and power on the V-IP .

Warning

The USB standard guarantees up to 500mA power per single USB port. The V-IP needs up to 700mA current and therefore does not work on USB alone. However, most of the current USB ports provide more than 700mA so that no external power is needed to power the V-IP . Taking more power from a USB port than specified may cause damage to your computer and is therefore not recommended.

Initial Network Configuration

Initially, the V-IP network interface is configured with the parameters shown in Table 1-1 .

Table 1-1. Initial Network Configuration

Parameter	Value
IP auto configuration	DHCP
IP address	-
Netmask	255.255.255.0
Gateway	none
IP access control	none

> **Warning**
>
> If the DHCP connection fails on boot up, the V-IP will not have an IP address.

If this initial configuration does not meet your local requirements, adjust the values to your needs. You may either configure the V-IP via serial interface, or use the setup tool that can be found on the CD ROM delivered with this package.

V-IP Setup Tool

Main Window

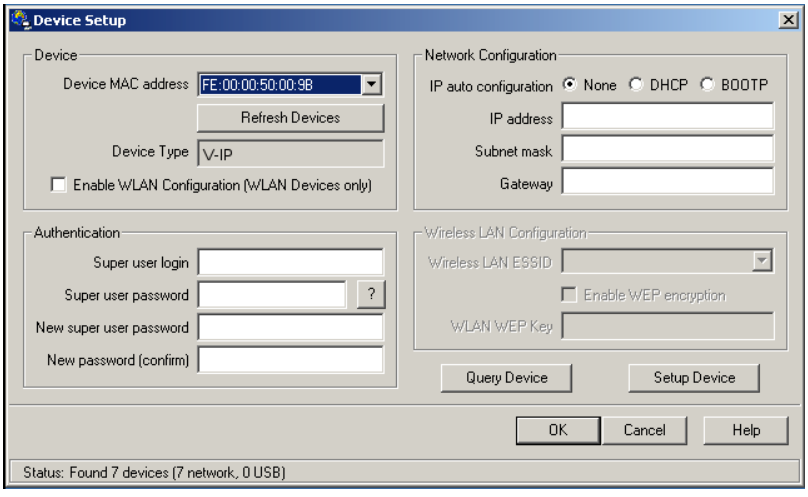

Figure 1-3. V-IP setup tool

Connect the V-IP to your computer either via local network or via USB. Start the setup tool from the CD ROM on the computer where the V-IP is installed. Depending on the connection (USB or network), the device detection is different. A window opens as seen in Figure 1-3 .

MAC Address Detection

On the upper left corner, the MAC address of the V-IP is displayed. To detect the MAC address manually, press the button " Refresh Devices " . The displayed MAC address is the same MAC address printed on the white sticker placed on the back of the V-IP . If the V-IP is connected via USB, it is classified as a USB device and an appropriate drive letter is chosen for this device. On the lower right corner of the window, there are two buttons: " Query Device " and " Setup Device " . Press the " Query Device " button to display the preconfig- ured values of the network configuration. The values are displayed in the text fields located above. If necessary, adjust the network settings to your needs. To save the changes enter a user name and an according password. Then press the " Setup De- vice " button.

Authentication

To adjust the authentication settings, enter your login as a superuser and change your password.

Super user login

Enter the login name of the super user. The initial value is " admin " .

Super user password

Enter the current password for the super user. This initial value is " hetec " .

New super user password

Enter the new password for the super user.

New password (confirm)

Re-type the new password for the super user.

To close the window and accept the changes press the " OK " button, otherwise press the " Cancel " button.

Configuration via Serial Interface

To configure the V-IP via serial interface both a serial port replicator cable and a null modem cable are required (available separately). Connect the enclosed Null Modem Cable to the serial interface with the black con- nector on the port replicator . The serial interface needs to be adjusted with the parameters as shown in Table 1-2 .

Table 1-2. Serial parameters

Parameter	Value
Bits/second	115200
Data bits	8
Parity	no
Stop bits	1
Flow control	none

Use a terminal software (e.g. `hyperterm` or `minicom`) to connect to the V-IP . Reset the V-IP , and immediately press the " ESC " key. You will see a " => " prompt. Enter the command " config " , and press the key " ENTER " . Quite soon afterwards you are asked to adjust the IP auto configuration, the IP address, the net mask, and the default gateway. Pressing the " ENTER " key without entering values does not change settings. The gateway value has to be set to `0.0.0.0` (for no gateway) or any other value for the IP address of the gateway. After the confirmation the V-IP performs a reset using the new values as set before.

Web Interface

The V-IP may be accessed using a standard Java enabled web browser. You may use the HTTP protocol or a secure encrypted connection via HTTPS. Just enter the configured IP address of the V-IP into your web browser. The initial login settings are:

Table 1-3. Standard User Settings

Parameter	Value
Login	admin
Password	hetec

Changing these settings to user specific values is strongly recommended and can be done on the " User Management " page (see the Section called Users And Groups in Chapter 6).

The Remote Console

The Remote Console is the redirected screen, keyboard and mouse of the remote host system in which the V-IP is installed. The web browser which is used for accessing the V-IP has to supply a Java Runtime Environment version 1.1 or higher. However, it is strongly recommended to install Sun JVM 1.4. The Remote Console will behave exactly the same way as if you were sitting directly in front of the screen of your remote system. That means that both the keyboard and mouse can be used in the usual way. Open the console by selecting the preview picture on the main site of the HTML frontend. Figure 1-4 shows the top of the Remote Console.

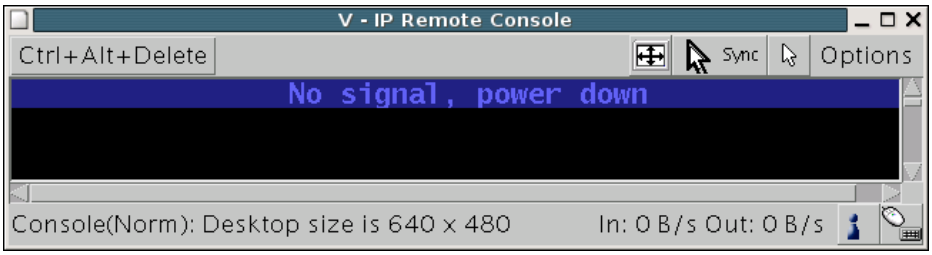

Figure 1-4. Top part of the Remote Console

There are some options to choose from the menu, the important ones are the following:

Auto Adjust button

If the video displayed is of bad quality or distorted in some way, press this button and wait a few seconds while the V-IP tries to adjust itself for the best possible video quality.

Sync Mouse

Choose this option in order to synchronize the local with the remote mouse cursor. This is especially necessary when using accelerated mouse settings on the host system. In general, there is no need to change mouse settings on that.

Video Settings in Options Menu

This opens a new window with elements to control the V-IP Video Settings. You can change some values, for instance related to brightness and contrast of the picture displayed, which may improve the video quality. It is also possible to revert to the default settings for all video modes or only the current one.

Note: At first start, if the local mouse pointer is not synchronized with the remote mouse pointer, press the Auto Adjust Button once.

Chapter 2. Introduction

Introduction

The V-IP is manufacturer-independent remote administration system. The V-IP works as an integrated solution on your server system. Based on an embedded operating system, the V-IP provides both exceptional stability and permanent availability independent of the present state of the server's operating system. As a system administrator, you have entire control and location-independent remote access to react upon both critical incidents and cases of necessary maintenance.

Figure 2-1. V-IP

Features

The V-IP defines a new class of remote access devices . It combines digital remote access via IP networks with comprehensive and integrated system management. The V-IP offers convenient, remote KVM access and control via LAN or Internet. It captures, digitizes, and compresses video and transmits it with keyboard and mouse signals to and from a remote computer. Remote access and control software runs on its embedded processors only but not on mission critical servers, so that there is no interference with server operation or impact on network performance. Furthermore, the V-IP offers additional remote power management with the help of optional available devices. Features of the V-IP are:

- KVM (keyboard, video, mouse) access over IP or analog telephone line
- No impact on server or network performance
- Automatically senses video resolution for best possible screen capture
- High-performance mouse tracking and synchronization
- Port to connect a user console for direct analogous access to KVM switch
- Local Mouse suppression (only when using SUN's Java Virtual Machine)

V-IP System Components

The V-IP is a stand alone product with the following dimensions:
95mm (D) x 25mm (H) x 72mm (W)
The V-IP is shipped with:

- a base unit
- an external power supply (HETEC SA-051A5F-12)
- a power cord
- a KVM cable
- transparent equipment feet
- an Installation and User Manual on a CD ROM
- a quick start guide
- a port replicator cable (VGA, PS/2, serial) (item #7020036)

Available separately (optional):

- an Inline Power Module IPM 220-L (item #8400400)

When the Server is up and running

The V-IP gives you full control over the remote server. The Management Console allows you to access the remote server's graphics, keyboard and mouse and to send special commands to the server. You can also perform periodic maintenance of the server. Using the Console Redirec- tion Service you can do the following:

- Reboot the system (a graceful shutdown)
- Watch the boot process
- Boot the system from a separate partition to load the diagnostic environment
- Run special diagnostic programs

When the Server is dead

Obviously, fixing hardware defects is not possible using a remote management device. Nevertheless, the V-IP gives the administrator valuable information about the type of a hardware failure. Serious hardware failures can be categorized into five different categories with dif- ferent chances to happen [1] :

Table 2-1. Hardware failures

Category	Probability
Hard disk failure	50%
Power cable detached, power supply failure	28%

Category	Probability
CPU, Controller, motherboard failure	10%
CPU fan failure	8%
RAM failure	4%

Using the V-IP , administrators can determine which kind of serious hardware failure has occurred (see Table 2-2).

Table 2-2. Host system failures and how they are detected

Type of failure	Detected by
Hard disk failure	Console screen, CMOS set-up information
Power cable detached, power supply failure	Server remains in power off state after power on command has been given.
CPU, Controller, main board failure	Power supply is on, but there is no video output.
CPU fan failure	By server specific management software
RAM failure	Boot-Sequence on boot console

Notes

1. According to a survey made by the Intel Corp.

Chapter 3. Installation

Operation Overview

The V-IP redirects local keyboard, mouse and video data to a remote administration console. All data is transmitted with the TCP/IP protocol family.

The V-IP can be used in both a multi-administrator and multi-server environment. Combining one or more V-IP s with a single KVM switch allows access to multiple servers on a single remote console.

Connectors and Jumpers

Front Side Connectors and Indicators

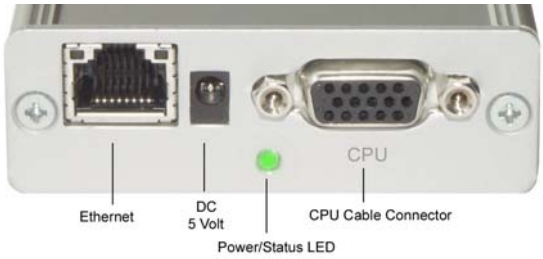

Figure 3-1. Front Side Connectors and Indicators

System port

Attach the system cable to this port.

Power/Status LED

Displays the status of the V-IP :

- LED off: the V-IP has no or not enough power
- LED blinking: the V-IP is booting up (if this process takes longer than one minute, the reason may be a lack of power).
- LED on: the V-IP is up and running.

If the V-IP is connected via USB only and the Power/Status LED tends not to stop blinking after one minute, the V-IP may not receive enough power via USB. In that case attach the enclosed power supply to the V-IP .

Power supply DC 5V

Attach the enclosed power supply to the V-IP .

- Voltage: 5V
- Current: 1.5 A

RJ45 Ethernet

UTP3/5 cables can be connected to the V-IP using this standard RJ45 jack.

Rear Side Connectors

Figure 3-2. Rear Side Connectors

Port replicator Here you may attach an optional port replicator enabling PS/2 support, serial and local console.

Connecting the V-IP to the Host System

Perform the following steps in order to connect the KVM signals of the server system to the V-IP :

1. Connect the pre-mounted system cable to
   - The VGA outlet of your server or the local console video port of your KVM switch.
   - The USB to one of the USB interfaces of your server or your USB-KVM switch.
2. Connect the RJ45 Ethernet connector to your local Ethernet hub using a CAT5 cable.
3. Connect the external power supply to the 5V power connector and power on the V-IP .

Warning

The USB standard guarantees up to 500mA power per single USB port. The V-IP needs up to 700mA current and therefore does not work on USB alone. However, most of the current USB ports provide more than 700mA so that no external power is needed to power the V-IP . Taking more power from a USB port than specified may cause damage to your computer and is therefore not recommended.

Connecting a Local Console

To connect a local console to the host system besides the V-IP you may attach a monitor, a keyboard and a mouse to the connectors on the port replicator .

Connecting Ethernet

The front side of the V-IP provides a RJ45 connector for Ethernet. The connector is used either for a 100 Mbps 100Base-TX connection or for a 10 Mbps 10BASE-T connection. The adapter can sense the connection speed and will adjust to the appropriate operation mode automatically.

10 Mbps Connection

For 10BASE-T Ethernet networks the Fast Ethernet adapter uses category 3, 4, or 5 UTP cable. To establish a 10 Mbps connection, the cable has to be connected to a 10BASE-T hub.

- Make sure that the cable is wired appropriately for a standard 10BASE-T adapter.
- Align the RJ45 plug with the notch on the adapter's connector and insert it into the adapter's connector.

100 Mbps Connection

For 100BASE-TX Ethernet networks the V-IP supports category 5 UTP cabling. To establish a 100 Mbps connection, the cable has to be connected to a 100BASE-TX hub.

- Make sure that the cable is wired appropriately for a standard 100BASE-TX adapter.
- Align the RJ45 plug with the notch on the adapter's connector and insert it into the adapter's connector.

Warning

The UTP wire pairs and configuration for 100BASE-TX cable are identical to those for 10BASE-T cable when used with category 5 UTP cable.

Chapter 4. Configuration

Initial Configuration

The V-IP 's communication interfaces are all based on TCP/IP. It comes pre-configured with the IP configuration listed in Table 4-1 .

Table 4-1. Initial network configuration

Parameter	Value
IP auto configuration	DHCP
IP address	-
Netmask	255.255.255.0
Gateway	none
IP access control	none

> **Warning**
>
> If the DHCP connection fails on boot up, the V-IP will not have an IP address.

If this initial configuration does not meet your requirements, the following describes the initial IP configuration that is necessary to access the V-IP for the first time.

V-IP Setup Tool

Main Window

Connect the V-IP to your computer either via local network or via USB. Start the setup tool from the CD ROM on the computer where the V-IP is installed. Depending on the connection (USB or network), the device detection is different. A window opens as seen in Figure 4-1 .

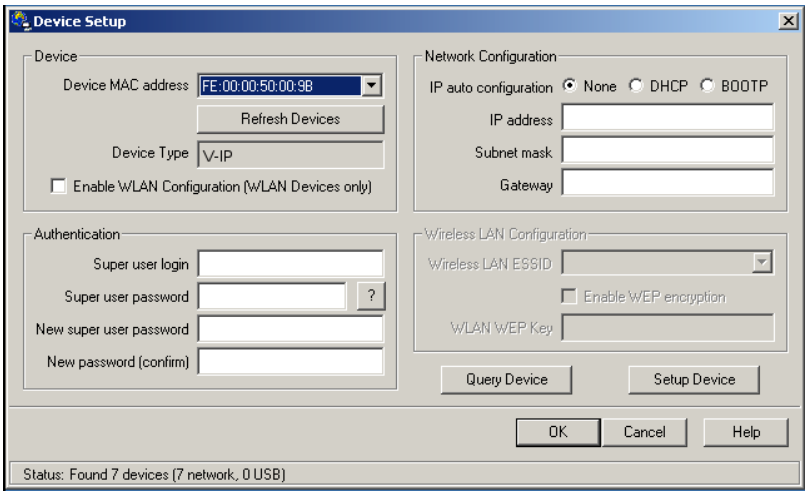

Figure 4-1. V-IP setup tool

MAC Address Detection

On the upper left corner, the MAC address of the V-IP is displayed. To detect the MAC address manually, press the button “ Refresh Devices ” . The displayed MAC address is the same MAC address printed on the white sticker placed on the back of the V-IP . If the V-IP is connected via USB, it is classified as a USB device and an appropriate drive letter is chosen for this device.
On the lower right corner of the window, there are two buttons: “ Query Device ” and “ Setup Device ” . Press the “ Query Device ” button to display the preconfigured values of the network configuration. The values are displayed in the text fields located above. If necessary, adjust the network settings to your needs. To save the changes enter a user name and an according password. Then press the “ Setup Device ” button.

Authentication

To adjust the authentication settings, enter your login as a superuser and change your password.

Super user login

Enter the login name of the super user. The initial value is “ admin ” .

Super user password

Enter the current password for the super user. This initial value is “ hetec ” .

New super user password

Enter the new password for the super user.

New password (confirm)

Re-type the new password for the super user.

To close the window and accept the changes press the “ OK ” button, otherwise press the “ Cancel ” button.

Initial Configuration via DHCP Server

By default, the V-IP will try to contact a DHCP server in the subnet to which it is physically connected. If a DHCP server is found, it may provide a valid IP address, gateway address and net mask. Before you connect the device to your local subnet, be sure to complete the corresponding configuration of your DHCP server. It is recommended to configure a fixed IP assignment to the MAC address of the V-IP . You can find the MAC address on the outside of the shipping box and labeled on the bottom side. If this initial configuration does not meet your local requirements, use the setup tool to adjust the values to your needs. The setup tool can be found on the CD ROM delivered with this package. You can follow the procedure described below.

Initial Configuration via Serial Console

To configure the V-IP via serial interface both a serial port replicator cable and a null modem cable are required .

Using a serial terminal, the V-IP has a serial line interface (rear side). This connector is compliant with the RS 232 serial line standard. To establish a serial connection use a standard NULL-Modem cable. The serial line has to be configured with the parameters given in Table 4-2 .

When configuring with a serial terminal, reset the V-IP and immediately press the " ESC " key. You will see a " => " prompt. Enter " config " , press " Enter " and wait for a few seconds for the configuration questions to appear.

Table 4-2. Serial line parameters

Parameter	Value
Bits/second	115200
Data bits	8
Parity	no
Stop bits	1
Flow control	none

As you proceed, the following questions will appear on the screen. To accept the default values which are shown in square brackets below, press " Enter " .

```
IP auto configuration (non/dhcp/bootp) [dhcp]:
IP [192.168.1.22]:
Net mask [255.255.255.0]:
Gateway (0.0.0.0 for none) [0.0.0.0]:
```

IP autoconfiguration

With this option you can specify whether the V-IP should get its network settings from a DHCP or BOOTP server. For DHCP, enter " dhcp " , and for BOOTP enter " bootp " . If you do not specify any of these, the IP autoconfiguration is disabled and subsequently you will be asked for the following network settings.

IP address

The IP address the V-IP uses. This option is only available if IP autoconfiguration is disabled.

Net mask

The net mask of the connected IP subnet. This option is only available if IP autoconfiguration is disabled.

Gateway address

The IP address of the default router for the connected IP subnet. If you do not have a default router, enter `0.0.0.0` . This option is only available if IP autoconfiguration is disabled.

Finally, you will be asked if the values are correct, and may adjust them if necessary. After your confirmation the V-IP performs a reset using the new values.

Web Interface

The V-IP may be accessed using a standard Java enabled web browser. You may use the HTTP protocol or a secure encrypted connection via HTTPS. Just enter the configured IP address of the V-IP into your web browser. The initial login settings are:

Table 4-3. Standard User Settings

Parameter	Value
Login	admin
Password	hetec

Changing these settings to user specific values is strongly recommended and can be done on the " User Management " page (see the Section called Users And Groups in Chapter 6).

Mouse, Keyboard and Video configuration

Between the V-IP and the host, there are two interfaces available for transmitting keyboard and mouse data: USB and PS/2 . The correct operation of the remote mouse depends on several settings which will be discussed in the following subsections.

V-IP USB interface

To use the USB interface a correct cabling between the managed host and the managing device is necessary. If the managed host has no USB keyboard support in the BIOS and you have connected the USB cable only, then you will have no remote keyboard access during the boot process of the host. Please see the Section called Keyboard/Mouse in Chapter 6 for more details.

V-IP Keyboard Settings

The V-IP settings for the host's keyboard type have to be correct in order to make the remote keyboard work properly. Check the settings in the V-IP front-end. See the Section called Keyboard/Mouse in Chapter 6 for details.

Remote Mouse Settings

A common problem with KVM devices is the synchronization between the local and remote mouse cursors. The V-IP addresses this situation with an intelligent synchronization algorithm. There are three mouse modes available on the V-IP .

Auto Mouse Speed

The automatic mouse speed mode tries to detect the speed and acceleration settings of the host system automatically. See the section below for a more detailed explanation.

Fixed Mouse Speed

This mode just translates the mouse movements from the Remote Console in a way that one pixel move will lead to n pixel moves on the remote system. This parameter n is adjustable with the scaling. It should be noted that this works only when mouse acceleration is turned off on the remote system.

Single/Double Mouse Mode

This mode is described in the Section called Single and Double Mouse Mode .

Auto Mouse Speed and Mouse Synchronization

The automatic mouse speed mode performs the speed detection during mouse synchronization. Whenever the mouse does not move correctly, there are two ways for re-synchronizing local and remote mouse:

Fast Sync

The fast synchronization is used to correct a temporary but fixed skew. Choose the option from the Remote Console options menu. If defined you may also press the mouse synchronization hotkey sequence (see the Section called Remote Console Control Bar in Chapter 5 for details).

Intelligent Sync

If the fast sync does not work or the mouse settings have been changed on the host system, use the intelligent resynchronization. This method takes more time than the fast one and can be accessed with the appropriate item in the Remote Console option menu. The intelligent synchronization requires a correctly adjusted picture. Use the auto adjustment function or the manual correction in the Video Settings panel to setup the picture. The Sync mouse button on top of the Remote Console can behave differently, depending on the current state of mouse synchronization. Usually pressing this button leads to a fast sync, except in situations where the video mode changed recently. See also the Section called Remote Console Control Bar in Chapter 5 .

Note: At first start, if the local mouse pointer is not synchronized with the remote mouse pointer, press the Auto Adjust Button once.

Host System Mouse Settings

The host's operating system knows various settings for the mouse driver.

Warning

The following limitations do not apply in case of USB and Mouse Type " MS Windows 2000 and newer " .

While the V-IP works with accelerated mice and is able to synchronize the local with the remote mouse pointer, there are the following limitations which may prevent this synchronization from working properly:

Special Mouse Driver

There are mouse drivers which influence the synchronization process and lead to desynchronized mouse pointers. If this happens, make sure you do not use a special vendor-specific mouse driver on your host system.

Windows 2003 Server/XP Mouse Settings

Windows XP knows a setting named " improve mouse acceleration " which has to be deactivated.

Active Desktop

If the Active Desktop feature of Microsoft Windows is enabled, do not use a plain background. Instead, use some kind of wallpaper. As an alternative, you could also disable the Active Desktop completely.

See also the Section called Recommended Mouse Settings for mouse mode recommendations.

Navigate your mouse pointer into the upper left corner of the applet screen and move it slightly forth and back. Thus the mouse will be resynchronized. If resynchronizing fails, disable the mouse acceleration and repeat the procedure.

Single and Double Mouse Mode

The information above applies to the Double Mouse Mode where remote and local mouse pointers are visible and need to be synchronized. The V-IP also features another mode, the Single Mouse Mode, where only the remote mouse pointer is visible. Activate this mode in the Remote Console (see the Section called Remote Console Control Bar in Chapter 5) and click into the window area. The local mouse pointer will be hidden and the remote one can be controlled directly. To leave this mode it is necessary to define a mouse hotkey in the Remote Console Settings Panel Press this key to free the captured local mouse pointer.

Recommended Mouse Settings

For the different operating systems we can give the following advice:

MS Windows NT4

NT4 supports PS/2, only. Please choose the options PS/2 mouse and Auto Mouse Speed.

MS Windows 2000, 2003, XP (all versions)

In general, we recommend the usage of a mouse via USB. Choose USB without Mouse Sync.

For a PS/2 mouse choose Auto Mouse Speed. For XP disable the option " enhance pointer precision " in the Control Panel.

Note: The remote mouse is always synchronized with the local mouse if selecting the option " MS Windows 2000 or newer " .

SUN Solaris

Adjust the mouse settings either via " xset m 1 " or use the CDE Control Panel to set the mouse to " 1:1, no acceleration " . As an alternative you may also use the Single Mouse Mode.

MAC OS X

We recommend using the Single Mouse Mode.

OS/2

We recommend using the Single Mouse Mode.

Linux First, choose the option " Other Operating Systems " from the the Mouse Type selection box. Second, choose the option Auto Mouse Speed. This applies for both USB and PS/2 mice.

Video Modes

The V-IP recognizes a limited number of common video modes. When running X11 on the host system please do not use any custom modelines with special video modes. If you do, the V-IP may not be able to detect them. We recommend using any of the standard VESA video modes instead. Please refer to Appendix C for a list of all supported video modes.

Resetting the V-IP to its Factory Settings

Using the Serial Interface

Reset the V-IP and immediately press the " ESC " key. On your screen a command prompt " => " will be visible. Enter " defaults " , press the " Enter " key and wait for a few seconds for the V-IP to reboot. Now, you may use the default settings as described in the Section called Initial Configuration .

Chapter 5. Usage

Prerequisites

The V-IP features an embedded operating system and applications offering a variety of standardized interfaces. This chapter will describe both these interfaces and the way to use them in a more detailed manner. The interfaces are accessed using the TCP/IP protocol family, thus they can be accessed using the built-in Ethernet adapter . The following interfaces are
supported:

HTTP/HTTPS

Full access is provided by the embedded web server. The V-IP environment can be entirely managed using a standard web browser. You can access the V-IP using the insecure HTTP protocol or using the encrypted HTTPS protocol. Whenever possible use HTTPS.

Telnet

A standard Telnet client can be used to access an arbitrary device connected to the V-IP 's serial port via a terminal mode.

The primary interface of the V-IP is the HTTP interface. This is covered extensively in this chapter. Other interfaces are addressed in subtopics.
In order to use the Remote Console window of your managed host system, the browser has to come with a Java Runtime Environment version 1.1 or higher. If the browser has no Java support (such as on a small handheld device), you are still able to maintain your remote host system using the administration forms displayed by the browser itself.

Important: We recommend to install a Sun JVM 1.4.

For an insecure connection to the V-IP we can recommend the following web browsers:

- Microsoft Internet Explorer version 5.0 or higher on Windows 98, Windows ME, Windows 2000 and Windows XP
- Netscape Navigator 7.0, Mozilla 1.6 and Mozilla Firefox on Windows 98, Windows ME, Windows 2000, Windows XP, Linux and other UNIX-like Operating Systems

In order to access the remote host system using a securely encrypted connection, you need a browser that supports the HTTPS protocol. Strong security is only assured by using a key length of 128 Bit. Some of the old browsers do not have a strong 128 Bit encryption algorithm. Using the Internet Explorer, open the menu entry " ? " and " Info " to read about the key length that is currently activated. The dialog box contains a link that leads you to information on how to upgrade your browser to a state of the art encryption scheme. Figure 5-1 shows the dialog box presented by the Internet Explorer 6.0.

Figure 5-1. The Internet Explorer displaying the encryption key length

Newer web browsers do support strong encryption on default.

Login into the V-IP and logout

Login into the V-IP

Open your web browser. Type in the address of your V-IP which you configured during the installation process. The address used might be a plain IP address or a host and domain name, in case you have given your V-IP a symbolic name in the DNS. For instance, type the following in the address line of your browser when establishing an unsecured connection:

```
http://192.168.1.22/
```

When using a secure connection type in:

```
https://192.168.1.22/
```

This will lead you to the V-IP login page as shown in Figure 5-2 .

Figure 5-2. Login screen

The V-IP has a built-in super user that has all permissions to administrate your V-IP :

Table 5-1. Standard User Settings

Parameter	Value
Login	admin
Password	hetec

Warning

The user “ admin ” is not allowed to login via the serial interface of the V-IP .

Warning

Please make sure to change the super user password immediately after you have installed and accessed your V-IP for the first time. Not changing the pass phrase for the super user is a severe security risk and might result in unauthorized access to the V-IP and to the host system including all possible consequences!

Warning

Your web browser has to accept cookies or else login is not possible.

Navigation

Having logged into the V-IP successfully, the main page of the V-IP appears (see Figure 5-3). This page consists of three parts, each of them contains specific information. The buttons on the upper side allow you to navigate within the front end (see Table 5-2 for details). The lower left frame contains a navigation bar and allows you to switch between the different sections of the V-IP . Within the right frame, task-specific information is displayed that depends on the section you have chosen before.

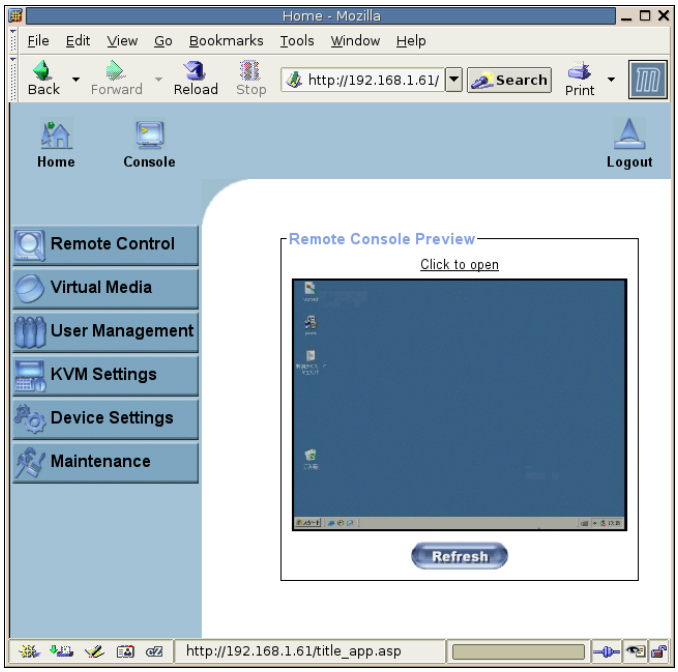

Figure 5-3. Main page

Table 5-2. Buttons from the front end

	Return to the main page of the V-IP .
	Open the V-IP Remote Console.
	Exit from the V-IP front end.

Warning

If there is no activity for half an hour, the V-IP will log you out automatically. A click on one of the links will bring you back to the login screen.

Logout from the V-IP

This link logs out the current user and presents a new login screen. Please note that an automatic logout will be performed in case there is no activity for half an hour.

The Remote Console

General Description

The Remote Console is the redirected screen, keyboard and mouse of the remote host system that V-IP controls.

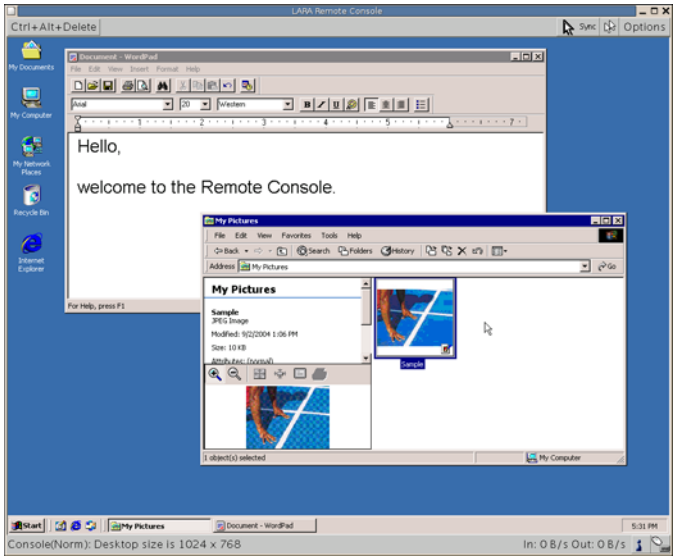

Figure 5-4. Remote Console

The Remote Console window is a Java Applet that tries to establish its own TCP connection to the V-IP . The protocol that is run over this connection is neither HTTP nor HTTPS, but RFB (Remote Frame Buffer Protocol). Currently RFB tries to establish a connection to port #443. Your local network environment has to allow this connection to be made, i.e. your firewall and, in case you have a private internal network, your NAT (Network Address Translation) settings have to be configured accordingly. In case the V-IP is connected to your local network environment and your connection to the Internet is available using a proxy server only without NAT being configured, the Remote Console is very unlikely to be able to establish the according connection. This is because today's web proxies are not capable of relaying the RFB protocol. In case of problems, please consult your network administrator in order to provide an appropriate network environment.

Main Window

Starting the Remote Console opens an additional window. It displays the screen content of your host system. The Remote Console will behave exactly in the same way as if you were sitting directly in front of the screen of your remote system. That means keyboard and mouse can be used in the usual way. However, be aware of the fact that the remote system will react to keyboard and mouse actions with a slight delay. The delay depends on the bandwidth of the line which you use to connect to the V-IP . With respect to the keyboard, the very exact remote representation might lead to some confusion as your local keyboard changes its keyboard layout according to the

remote host system. If you use a German administration system and your host system uses a US English keyboard layout, for instance, special keys on the German keyboard will not work as expected. Instead, the keys will result in their US English counterpart. You can circumvent such problems by adjusting the keyboard of your remote system to the same mapping as your local one. The Remote Console window always tries to show the remote screen with its optimal size. That means it will adapt its size to the size of the remote screen initially and after the screen resolution of the remote screen has been changed. However, you can always resize the Remote Console window in your local window system as usual.

Warning

In difference to the remote host system, the Remote Console window on your local window system is just one window among others. In order to make keyboard and mouse work, your Remote Console window must have the local input focus.

Remote Console Control Bar

The upper part of the Remote Console window contains a control bar. Using its elements you can see the status of the Remote Console and influence the local Remote Console settings. A description for each control follows.

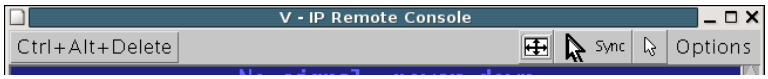

Figure 5-5. Remote Console Control Bar

Ctrl+Alt+Delete

Special button key to send the “ Control Alt Delete ” key combination to the remote system (see also the Section called KVM Settings in Chapter 6 for defining new button keys).

Note: For the user “ admin ” this button exists on default. Other users have to define this button on their own.

Auto Adjust button

If the video displayed is of bad quality or distorted in some way, press this button and wait a few seconds while the V-IP tries to adjust itself for the best possible video quality.

Sync Mouse

Choose this option in order to synchronize the local with the remote mouse cursor. This is especially necessary when using accelerated mouse settings on the host system. In general, there is no need to change mouse settings on that.

Single/Double Mouse mode

Switches between the Single Mouse Mode (where only the remote mouse pointer is visible) and the Double Mouse Mode (where remote and local mouse pointers are visible and need to be synchronized). Single mouse mode is only available if using SUN JVM 1.4 or higher.

Options

To open the Options menu click on the button “ Options ” .

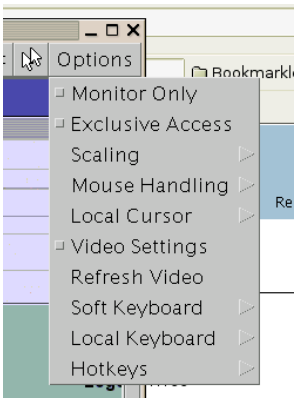

Figure 5-6. Remote Console Options Menu

A short description of the options follows.

- Monitor Only

  Toggles the Monitor Only filter on or off. If the filter is switched on no remote console interaction is possible, and monitoring is possible.

- Exclusive Access

  If a user has the appropriate permission, he can force the Remote Consoles of all other users to close. No one can open the Remote Console at the same time again until this user disables the exclusive access or logs off.

  Note: This option is only accessible for the administrator and the admin .

  A change in the access mode is also visible in the status line. See the Section called Remote Console Status Line for more information.

- Scaling

  Allows you to scale down the Remote Console. You can still use both mouse and keyboard, however the scaling algorithm will not preserve all display details.

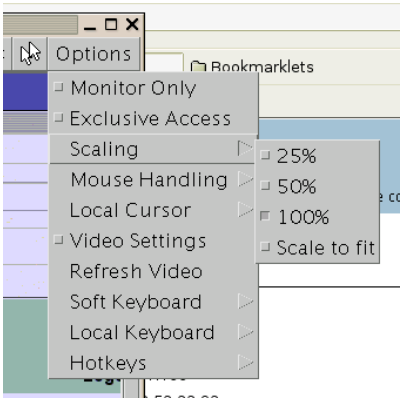

Figure 5-7. Remote Console Options Menu: Scaling

- Mouse Handling

  The submenu for mouse handling offers two options for synchronizing the local and the remote mouse pointer as explained in the Section called Mouse, Keyboard and Video configuration in Chapter 4 .

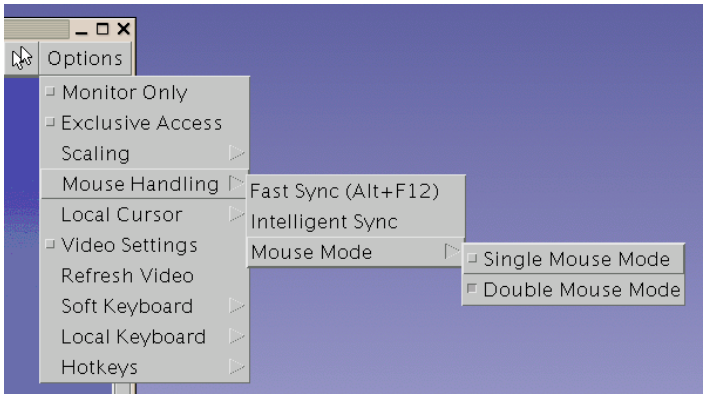

Figure 5-8. Remote Console Options Menu: Mouse Handling

- Fast Sync

  The fast synchronization is used to correct a temporary but fixed skew.

- Intelligent Sync

  Use this option if the fast sync does not work or the mouse settings have been changed on the host system.

> **Warning**
>
> This method takes more time than the fast one and requires a correctly adjusted picture. To setup the picture you may use either the auto adjustment function or the manual correction in the Video Settings panel .

- Local Cursor

  Offers a list of different cursor shapes to choose from for the local mouse pointer. The selected shape will be saved for the current user and activated the next time this user opens the Remote Console. The number of available shapes depends on the Java Virtual Machine, a version of 1.2 or higher offers the full list.

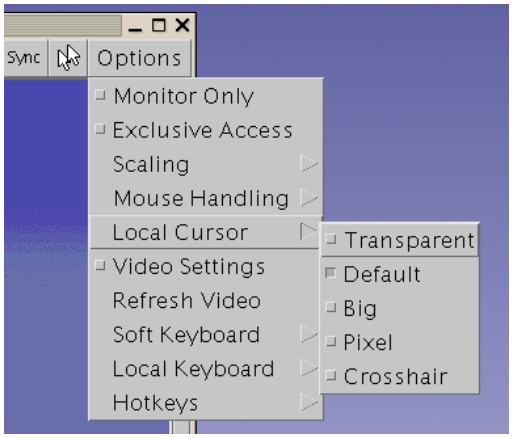

Figure 5-9. Remote Console Options Menu: Cursor

- Video Settings

  Opens a panel for changing the V-IP video settings. The V-IP features two different dialogs which influence the video settings.

  Video Settings through the HTML Frontend

  Select this option to enable local video port. This option decides if the local video output of the V-IP is active and passing through the incoming signal from the host system.

  The option Noise Filter defines how the V-IP reacts to small changes in the video input signal. A large filter setting needs less network traffic and leads to a faster video display but small changes in some display regions may not be recognized immediately. A small filter displays all changes instantly but may lead to a constant amount of network traffic even if display content is not really changing (depending on the quality of the video input signal). All in all the default setting should be suitable for most situations.

Video Settings through the remote console

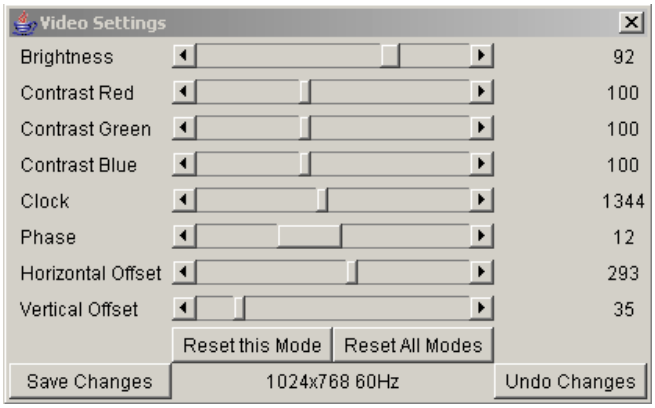

Figure 5-10. Video Settings Panel

Brightness

Controls the brightness of the picture.

Contrast

Controls the contrast of the picture.

Clock

Defines the horizontal frequency for a video line and depends on the video mode. Different video card types may require different values here. The default settings in conjunction with the auto adjustment procedure should be adequate for all common configurations. To achieve a better picture quality you may try to change this setting together with the sampling phase.

Phase

Defines the phase for video sampling, used to control the display quality together with the setting for sampling clock.

Horizontal Position

Use the left and right buttons to move the picture in horizontal direction while this option is selected.

Vertical Position

Use the left and right buttons to move the picture in vertical direction while this option is selected.

Reset this Mode

Reset mode specific settings to the factory-made defaults.

Reset all Modes

Reset all settings to the factory-made defaults.

Save changes

Save changes permanently.

Undo Changes

Restore last settings.

Note: This option is only available for the user “ admin ” .

- Refresh Video

  Use this option to refresh the video picture.

- Soft Keyboard

  Opens up the Menu for the Soft-Keyboard.

Figure 5-11. Soft Keyboard

- Show

  Pops up the Soft-Keyboard. The Soft-Keyboard is necessary in case your host system runs a completely different language and country mapping than your administration machine.

- Mapping

  Used for choosing the according language and country mapping of the Soft-Keyboard.

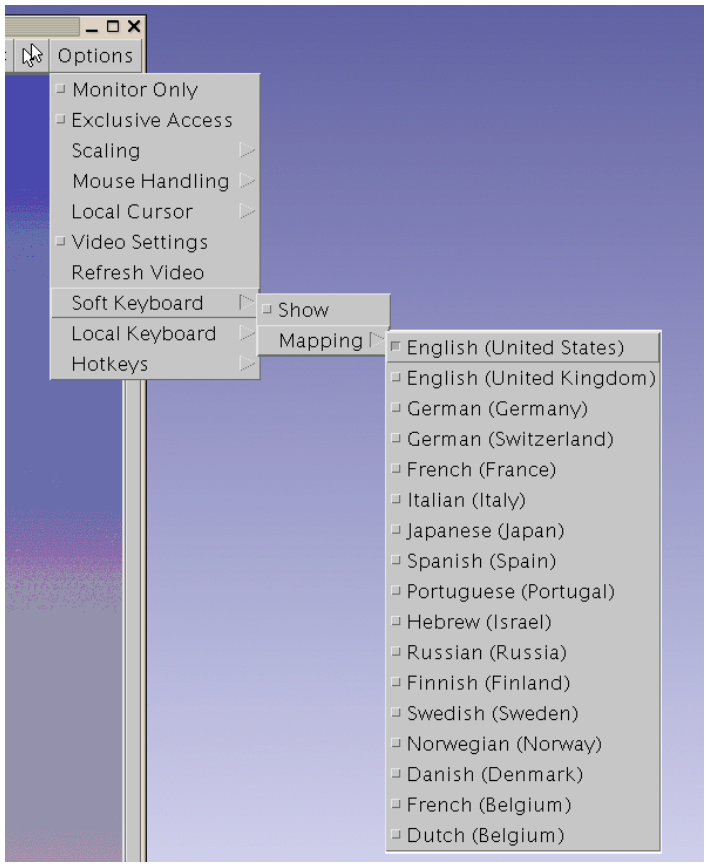

Figure 5-12. Soft Keyboard Mapping

- Local Keyboard

  Used to change the language mapping of your browser machine running the Remote Console Applet. Normally, the applet determines the correct value automatically. However, depending on your particular JVM and your browser settings this is not always possible. A typical example is a German localized system that uses a US-English keyboard mapping. In this case you have to change the Local Keyboard setting to the right language manually.

- Hotkeys

  Opens a list of hotkeys defined before. Choose one entry, the command will be sent to the host system. A confirmation dialog can be added that will be displayed before sending the selected command to the remote host. Select " OK " to perform the command on the remote host.

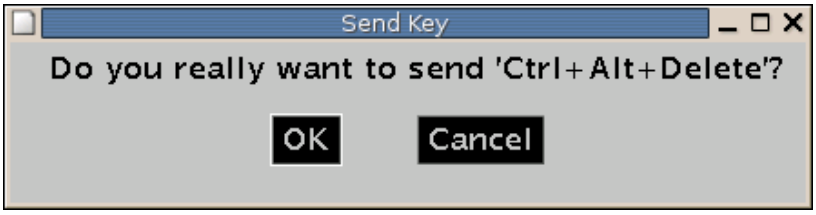

Figure 5-13. Remote Console Confirmation Dialog

Remote Console Status Line

The status line shows both console and the connection state. On the left the size of the remote screen is displayed. Figure 5-14 was taken from a Remote Console with a resolution of 800x600 pixels (see Appendix C for a list of screen resolutions that can be displayed using the V-IP). The value in brackets describes the connection to the Remote Console. “ Norm ” means a standard connection without encryption, “ SSL ” indicates a secure connection using SSL.

Figure 5-14. Status line

Furthermore, both the incoming (“ In: ”) and the outgoing (“ Out: ”) network traffic is visible (in kB/s). If compressed encoding is enabled, a value in brackets displays the compressed transfer rate.

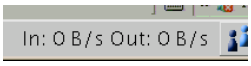

Figure 5-15. Status line transfer rate

The next button displays the Remote Console Access settings.

Table 5-3. Buttons displaying the access state

	One single user is connected to the Remote Console of the V-IP .
	One or more users are connected to the Remote Console of the V-IP .
	Exclusive access is set for you. Any other user may not access the remote host via Remote Console unless you disable this option.
	A remote user has exclusive access. You may not access the remote host via Remote Console unless the other user disables this option.

The outer right button displays the state of the Monitor Only settings.

Table 5-4. Buttons displaying the Monitor Only state

	The option Monitor Only is disabled.
	The option Monitor Only is enabled. For more information about Monitor Only and Exclusive Access settings see the ac- cording sections in the Section called Remote Console Control Bar .

Chapter 6. Menu Options

Remote Control

KVM Console

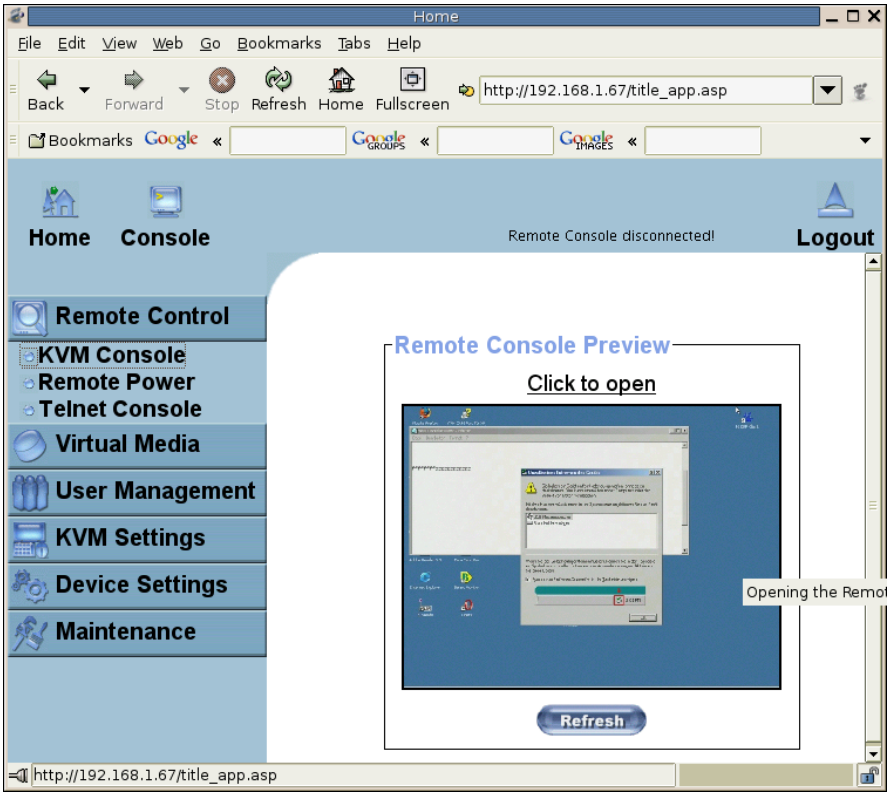

Figure 6-1. KVM Console

Remote Console Preview

To open the KVM console either click on the menu entry on the left or on the console picture on the right. To refresh the picture click on the button that is named “ Refresh ” .

Telnet Console

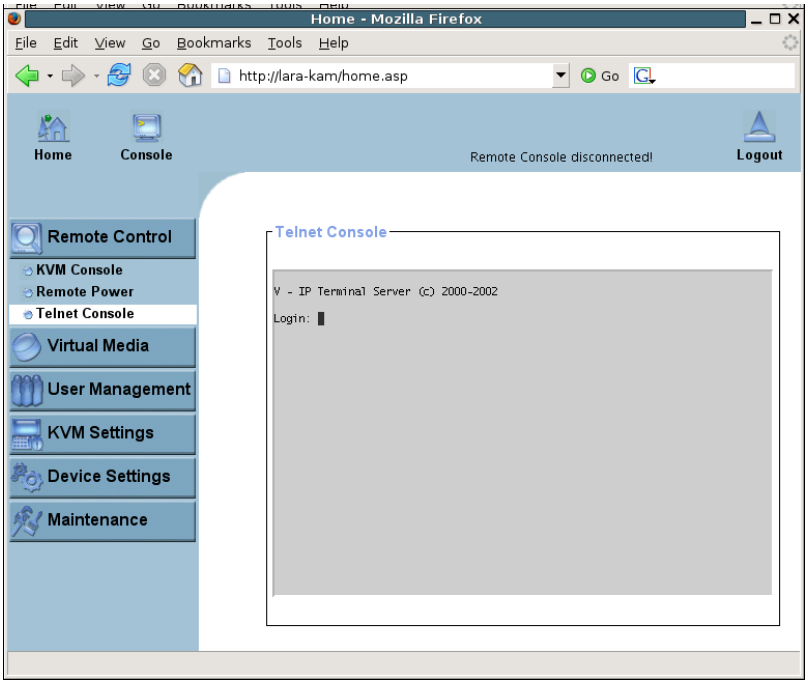

Figure 6-2. Telnet Console

The V-IP firmware features a Telnet gateway that enables a user to connect to the V-IP via a standard Telnet client.

For connecting to the V-IP via Telnet protocol you may use a terminal program such as `xterm` , `TeraTerm` or `Putty` . As an alternative you may also enter the `telnet` command on the command line or use the “ Run ” dialog from the Windows Start Menu. As an example you may type the following sequence:

```
telnet 192.168.1.22
```

Replace the IP address by the one that is actually assigned to the V-IP . This will prompt for user name and password in order to log into the device. The credentials that need to be entered for authentication are identical to those of the web interface. That means the user management of the Telnet interface is entirely controlled with the according functions of the web interface.
Once you have successfully logged into the V-IP a command line will be presented and you can enter the according management commands.
In general, the Telnet interface supports two operation modes: the command line mode and the terminal mode. The command line mode is used to control or display some parameters. In terminal mode the pass-through access to serial port 1 is activated (if the serial settings were made accordingly). To access the V-IP via serial interface both a serial port replicator cable and a null modem cable are required . All inputs are redirected to the device on serial port #1 and its answers are displayed on the Telnet interface.

The following list shows the command syntax and their usage.

help

Displays the list of possible commands

cls

Clears the screen

quit

Exits the current session and disconnects from the client

version

Displays the release information

terminal

Starts the terminal pass-through mode for serial port #1. The key sequence `esc exit` switches back to the command mode. The command has an optional parameter (1 or 2) to select the desired serial port for pass-through access.

Virtual Media

Floppy Disk

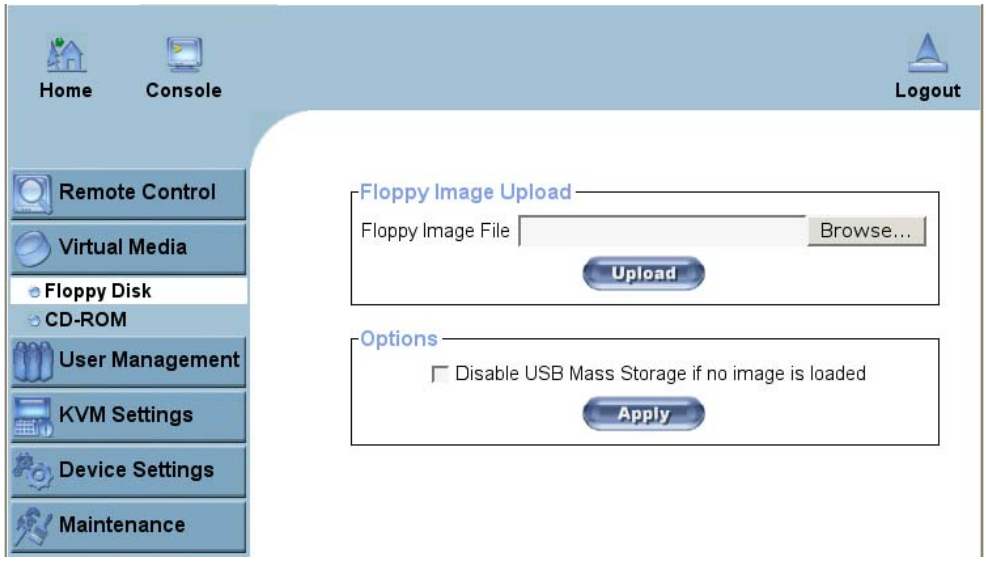

Figure 6-3. Virtual Floppy Area

Upload a Floppy Image

Within two small steps working on the basis of a certain (floppy) image can be achieved.

- First the path of the image has to be specified. You can do that either by hand or

by using the file selection dialog of your web browser. To open the file selection dialog click on the button “ Browse ” and select the desired image file.

Figure 6-4. Select Image File

The maximum image size is limited to 1.44MB. To use a larger image mount this image via Windows Share (or SAMBA) (see the Section called Use Image on Windows Share (SAMBA) for details).

- Secondly, click on the button “ Upload ” to initiate the transfer of the chosen image file into the V-IP ’s on-board memory. This image file is kept in the on-board memory of the V-IP until the end of the current session, until you logged out or initiated a reboot of the V-IP .

Options

Figure 6-5. USB mass storage option

Set this option to disable the mass storage emulation (and hide the virtual drive) if no image file is currently loaded. If unset and no file image will be found, it may happen that the host system will hang on boot due to changes in the boot order or the boot manager (LILO, GRUB). This case was reported for some Windows versions (2000, XP), other OS may not be fully excluded. This behaviour depends on the BIOS version used in that machine. To set this
option press the button “ Apply ” .

CD ROM

Use Image on Windows Share (SAMBA)

To include an image from a Windows share select “ CD-ROM ” from the submenu.

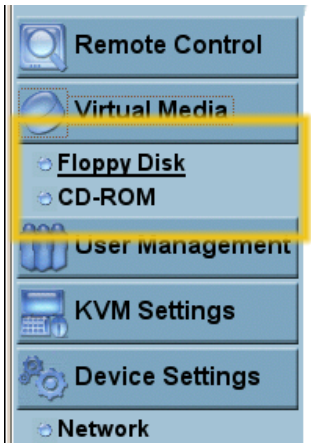

Figure 6-6. Selecting CD ROM

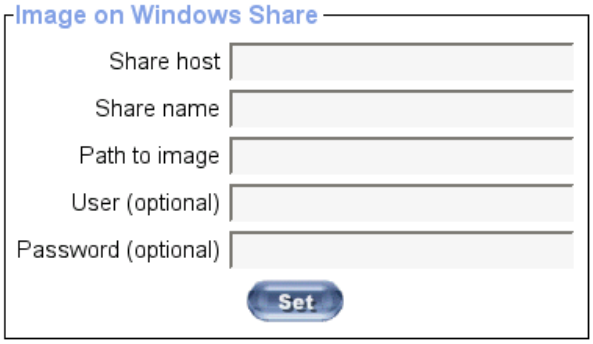

Figure 6-7. Select Windows Share

The following information has to be given to mount the image properly:

Share host

The server name or its IP address. On Windows 95, 98 and Windows ME do not specify the IP address but the server name (“ NetBIOS Name ”).

Share name

The name of the share to be used.

Path to image

The path of the image file on the share.

User (optional)

If necessary, specify the user name for the share named before. If unspecified and a guest account is activated, this guest account information will be used as your login.

Password (optional)

If necessary, specify the password for the given user name.

To register the specified file image and its location click on the button “ Set ” .
The specified image file is supposed to be accessible from the V-IP . The information above has to be given from the point of view of the V-IP . It is important to specify correct IP addresses and device names. Otherwise, the V-IP may not be able to access the referenced image file.
Furthermore, the specified share has to be configured correctly. Therefore, administrative permissions are required. As a regular user you may not have these permissions. You should either login as a system administrator (or as “ root ” on UNIX systems) or ask your system administrator for help to complete this task.

Windows 2000/XP

Open the Explorer, navigate to the directory (or share) and press the right mouse button to open the context menu.

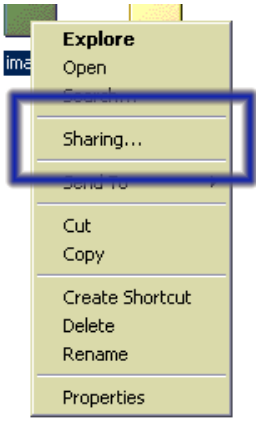

Figure 6-8. Explorer Context Menu

Select “ Sharing ” to open the configuration dialog.

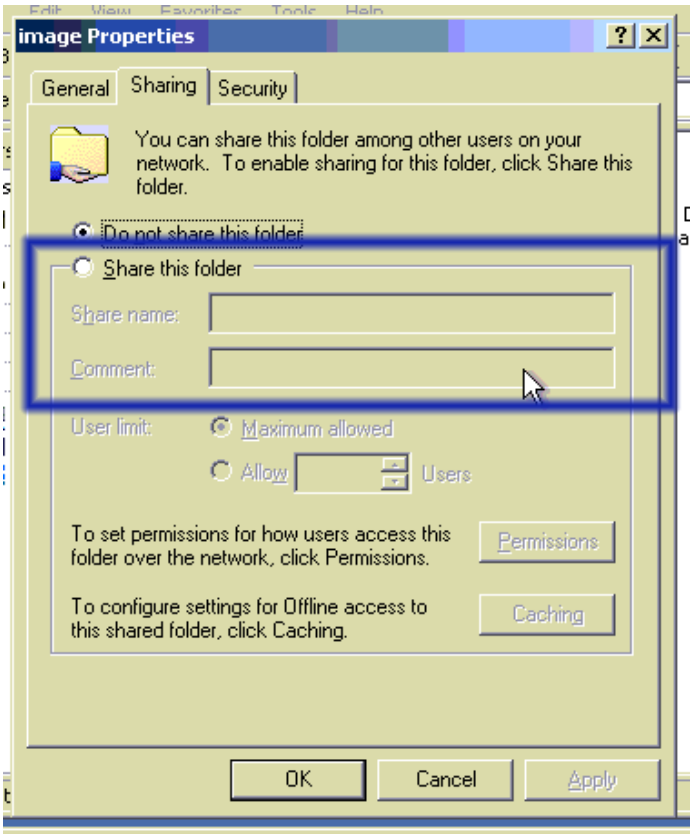

Figure 6-9. Share configuration dialog

Adjust the settings for the selected directory.

- Activate the selected directory as a share. Select " Sharing this folder " .
- Choose an appropriate name for the share. You may also add a short description for this folder (input field " Comment ").
- If necessary, adjust the permissions (button " permissions ").
- Click " OK " to set the options for this share.

UNIX and UNIX-like OS (UNIX, Solaris, Linux)

If you like to access the share via SAMBA, SAMBA has to be set up properly. You may either edit the SAMBA configuration file `/etc/samba/smb.conf` or use the Samba Web Administration Tool (SWAT) or WebMin to set the correct parameters.

For additional options see the Section called Options for details.

Creating an Image

Floppy Images

UNIX and UNIX-like OS To create an image file make use of “ dd ” . This is one of the original UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, Linux). To create a floppy image file copy the contents of a floppy to a file. You can use the following command:

dd [`if=/dev/fd0`] [`of=/tmp/floppy.image`] dd reads the entire disc from the device `/dev/fd0` and saves the output in the specified output file `/tmp/floppy.image` . Adjust both parameters exactly to your needs (input device etc.)

MS Windows

You can use the tool “ RawWrite for Windows ” .

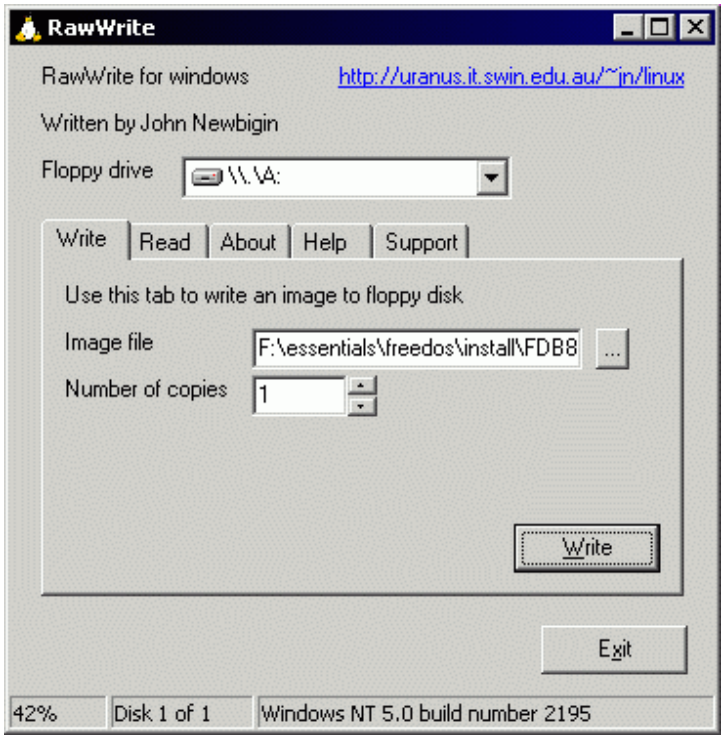

Figure 6-10. RawWrite for Windows selection dialog

Select the tab “ Read ” from the menu. Enter (or choose) the name of the file in which you would like to save the floppy content. Click on the button “ Copy ” to initiate the image creation process. For related tools you may have a look at the homepage of the fdos project (`http://www.fdos.org/ripcord/rawrite/`).

CD ROM/ISO 9660 Images

UNIX and UNIX-like OS To create an image file make use of “ dd ” . This is one of the original UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, Linux). To create a CDROM image file copy the contents of the CDROM to a file. You can use the following command:

dd [`if=/dev/cdrom`] [`of=/tmp/cdrom.image`] dd reads the entire disc from the device `/dev/cdrom` and saves the output in the specified output file `/tmp/cdrom.image` . Adjust both parameters exactly to your needs (input device etc.).

MS Windows To create the image file use your favourite CD imaging tool. Copy the whole contents of the disc into one single ISO image file on your harddisk. For example, with “ Nero ” you choose “ Copy and Backup ” . Then, navigate to the “ Copy Disc ” section. Select the CD ROM or DVD drive you would like to create an ISO image from. Specify the filename of the ISO image and save the CD ROM content in that file.

Figure 6-11. Nero selection dialog

User Management

Change Password

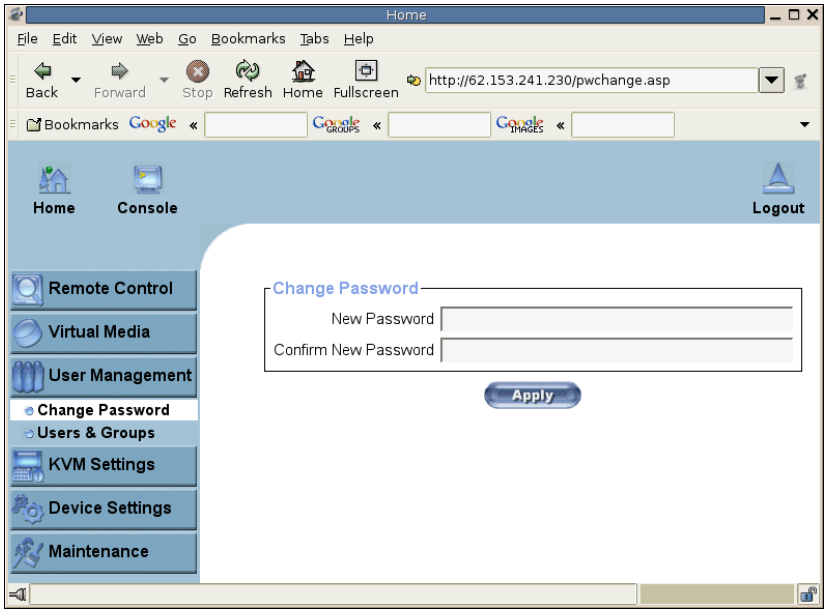

Figure 6-12. Set password

To change your password enter the new password in the upper entry field. Retype the password in the field below.

Click “ Apply ” to submit your changes.

Users And Groups

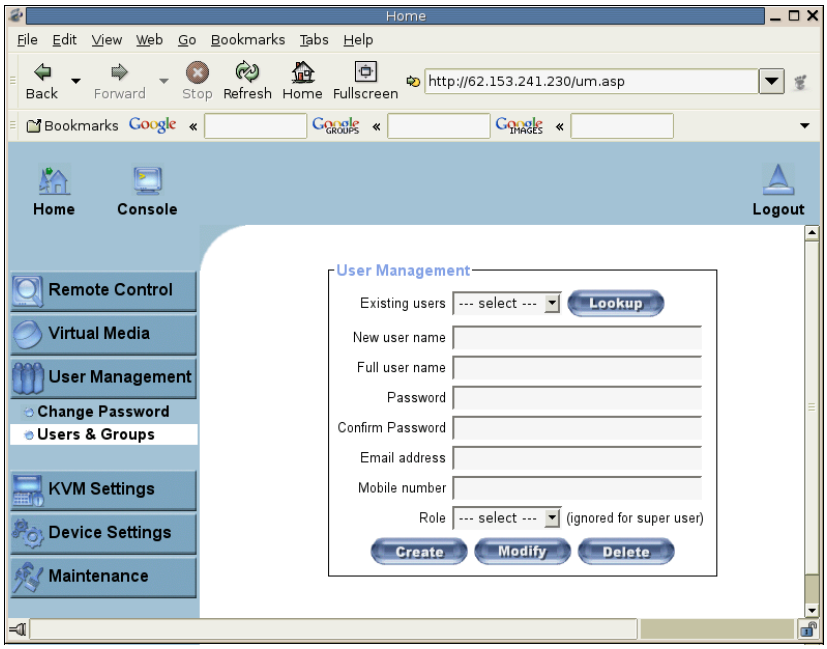

Figure 6-13. Set User

User Management

The V-IP comes with a pre-configured user account for the user “ admin ” that has fixed permissions. This user has all possible rights to configure the device and to use all functions the V-IP offers. Upon delivery, the account for the user “ admin ” has the password “ hetec ” . Make sure to change the password immediately after you have installed and firstly ac- cessed your V-IP . A full list of available options follows. This list can only be seen by the superuser.

Existing users

Select an existing user for modification. Once a user has been selected, click the lookup button to see the user information.

New User name

The new user name for the selected account.

Password

The password for the login name. It must be at least four characters long.

Confirm password

Confirmation of the password above.

Email address

This is optional.

Mobile number

This information may be optionally provided.

Note: The number of user profiles is limited to 150. The number of users that make use of the V-IP at the same time should not exceed the value of 25.

KVM Settings

User Console

The following settings are user specific. That means the super user can customize these settings for every users separately. Changing the settings for one user does not affect the settings for the other users.

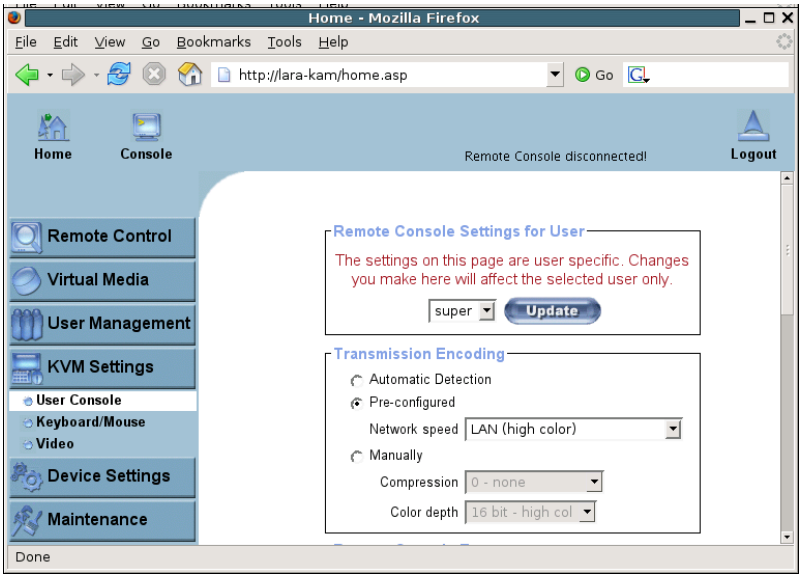

Figure 6-14. User Console Settings (Part 1)

Remote Console Settings for User

This selection box displays the user ID for which the values are shown and for which the changes will take effect. Select the desired user from the selection box and press the button “ Update ” . This will result in displaying the according user settings below.

Note: You are allowed to change the settings of other users only if you have the necessary access rights for this task. For a regular user without the correct permissions it is not possible to change the settings for any other users.

Transmission Encoding

The Transmission Encoding setting allows changing the image-encoding algorithm that is used to transmit the video data to the Remote Console window. It is possible to optimize the speed of the remote screen depending on the number of users working at the same time and the bandwidth of the connection line (Modem, ISDN, DSL, LAN, etc.).

Automatic detection

The encoding and the compression level is determined automatically from the available bandwidth and the current content of the video image.

Pre-configured

The pre-configured settings deliver the best result because of optimized adjustment of compression and colour depth for the indicated network speed.

Manually

Allows to adjust both compression rate and the colour depth individually. Depending on the selected compression rate the data stream between the V-IP and the Remote Console will be compressed in order to save bandwidth. Since high compression rates are very time consuming, they should not be used while several users are accessing the V-IP simultaneously. The standard colour depth is 16 Bit (65536 colours). The other colour depths are intended for slower network connections in order to allow a faster transmission of data. Therefore compression level 0 (no compression) uses only 16 Bit colour depth. At lower bandwidths only 4 Bit (16 colours) and 2 Bit (4 gray scales) are recommended for typical desktop interfaces. Photo-like pictures have best re- sults with 4 Bit (16 gray scales). 1 Bit colour depth (black/white) should only be used for extremely slow network connections.

Remote Console Type

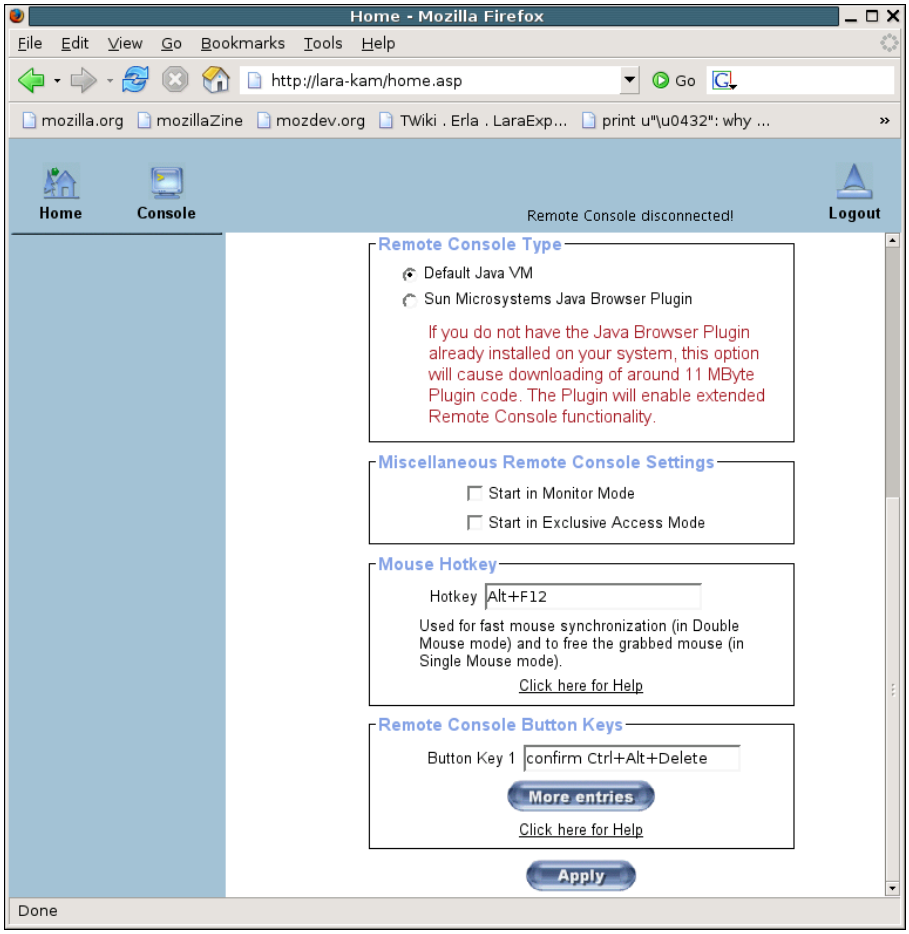

Figure 6-15. User Console Settings (Part 2)

Specifies which Remote Console Viewer to use.

Default Java Virtual Machine (JVM)
: Uses the default JVM of your web browser. This may be the Microsoft JVM for the Internet Explorer or the Sun JVM if it is configured this way. Use of the Sun JVM may also be forced (see below).

Sun Microsystems Java Browser Plugin
: Instructs the web browser of your administration system to use the JVM of Sun Microsystems. The JVM in the browser is used to run the code for the Remote Console window which is actually a Java Applet. If you check this box for the first time on your administration system and the appropriate Java plug-in is not yet installed on your system, it may be downloaded and installed automatically. However, in order to make the installation possible, you still have to answer the according dialogs with " yes " . The download volume is around 11 Mbytes. The advantage of downloading Sun's JVM is the usage of a stable and identical JVM across different platforms. The Remote Console software is optimized for this JVM version and offers a wider range of functionality when run in SUN's JVM.

(Hint: If you are connected over a slow connection to the Internet you can also pre-install the JVM on your administration machine.)

Miscellaneous Remote Console Settings

Start in Monitor Mode

Sets the initial value for the monitor mode. By default the monitor mode is disabled. In case you switch it on, the Remote Console window will be started in a read only mode.

Start in Exclusive Access Mode

Enables the exclusive access mode immediately at Remote Console startup. This forces the Remote Consoles of all other users to close. Nobody else can open the Remote Console at the same time again until you disable this feature or log off.

Mouse Hotkey

Allows to specify a hotkey combination which starts either the mouse synchronization process if pressed in the Remote Console or is used to leave the single mouse mode.

Remote Console Button Keys

Button Keys allow simulating keystrokes on the remote system that cannot be generated locally. The reason for this might be a missing key or the fact that the local operating system of the Remote Console is unconditionally catching this keystroke already. Typical examples are " Control+Alt+Delete " on Windows and DOS, what is always caught, or " Control+Backspace " on Linux for terminating the X-Server. The syntax to define a new Button Key is as follows:

```
[confirm] <keycode>[+|-[*]<keycode>]*
```

" confirm " requests confirmation by a dialog box before the key strokes will be sent to the remote host.

" keycode " is the key to be sent. Multiple key codes can be concatenated with a plus or a minus sign. The plus sign builds key combinations, all keys will be pressed until a minus sign or the end of the combination is encountered. In this case all pressed keys will be released in reversed sequence. So the minus sign builds single, separate keypresses and -releases. The star inserts a pause with a duration of 100 milliseconds. For a list of key codes and aliases the V-IP recognizes refer to Appendix E .

Note: If you need more button keys than shown use the button " More entries " . This will open a list of additional entry fields.

Keyboard/Mouse

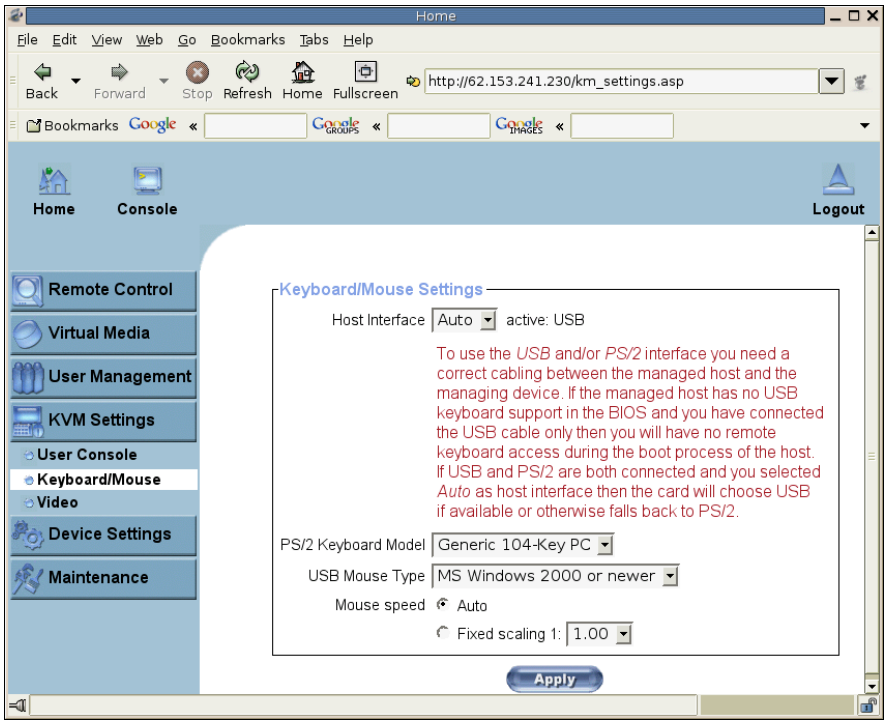

Figure 6-16. Keyboard and Mouse Settings

Host Interface

Enables a certain interface the mouse is connected to. You can choose between “ Auto ” for automatic detection, “ USB ” for a USB mouse and “ PS/2 ” for a PS/2 mouse.

> **Warning**
>
> To use the USB and/or PS/2 interface you need a correct cabling between the managed host and the managing device. If the managed host has no USB keyboard support in the BIOS and you have connected the USB cable only then you will have no remote keyboard access during the boot process of the host. If USB and PS/2 are both connected and you selected “ Auto ” as host interface, then the card will select “ USB ” if available or otherwise falls back to “ PS/2 ” .

To get USB remote keyboard access during the boot process of the host, the following conditions must be fulfilled:

- the host BIOS must have USB keyboard support
- the USB cable must be connected or must be selected in the Host interface option

PS/2 Keyboard Model

Enables a certain keyboard layout. You can choose between “ Generic 101-Key PC ” for a standard keyboard layout, “ Generic 104-Key PC ” for a standard keyboard layout extended by three additional Windows keys, “ Generic 106-Key PC ” for a Japanese keyboard, and “ Apple Macintosh ” for the Apple Macintosh.

USB Mouse Type

Enables the USB mouse type. Choose an appropriate option from the selection box. For a detailed description about the mouse type and recommended options for the different operating systems see the Section called Recommended Mouse Settings in Chapter 4 .

Mouse Speed

- Auto mouse speed
  Use this option if the mouse settings on the host use an additional acceleration setting. The V-IP tries to detect the acceleration and speed of the mouse during the mouse sync process.
- Fixed mouse speed

Use a direct translation of mouse movements between the local and the remote pointer. You may also set a fixed scaling which determines the amount the remote mouse pointer is moved when the local mouse pointer is moved by one pixel. This option only works when the mouse settings on the host are linear. This means that there is no mouse acceleration involved.

To set the options click on the button “ Apply ” .

Video

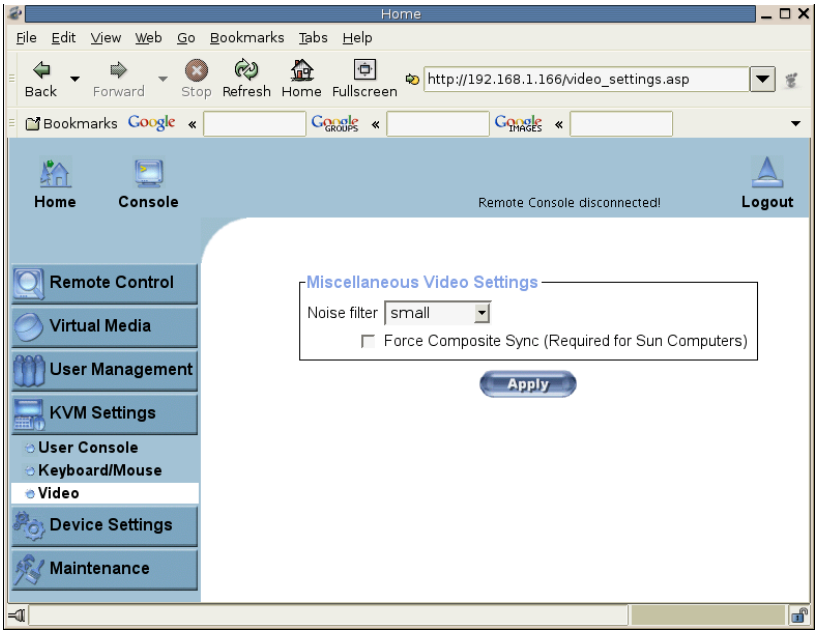

Figure 6-17. Video Settings

To set the options (see below) click on the button “ Apply ” .

Miscellaneous Video Settings

Noise filter

This option defines how the V-IP reacts to small changes in the video input signal. A large filter setting needs less network traffic and leads to a faster video display, but small changes in some display regions may not be recognized immediately. A small filter displays all changes instantly but may lead to a constant amount of network traffic even if the display content is not really changing (depending on the quality of the video input signal). All in all the default setting should be suitable for most situations.

Force Composite Sync (Required for Sun Computers)

To support signal transmission from a Sun machine enable this option. If not enabled the picture of the remote console will not be visible.

Device Settings

Network

The Network Settings panel as shown in Figure 6-18 allows changing network related parameters. Each parameter will be explained below. Once applied the new network settings will immediately come into effect.

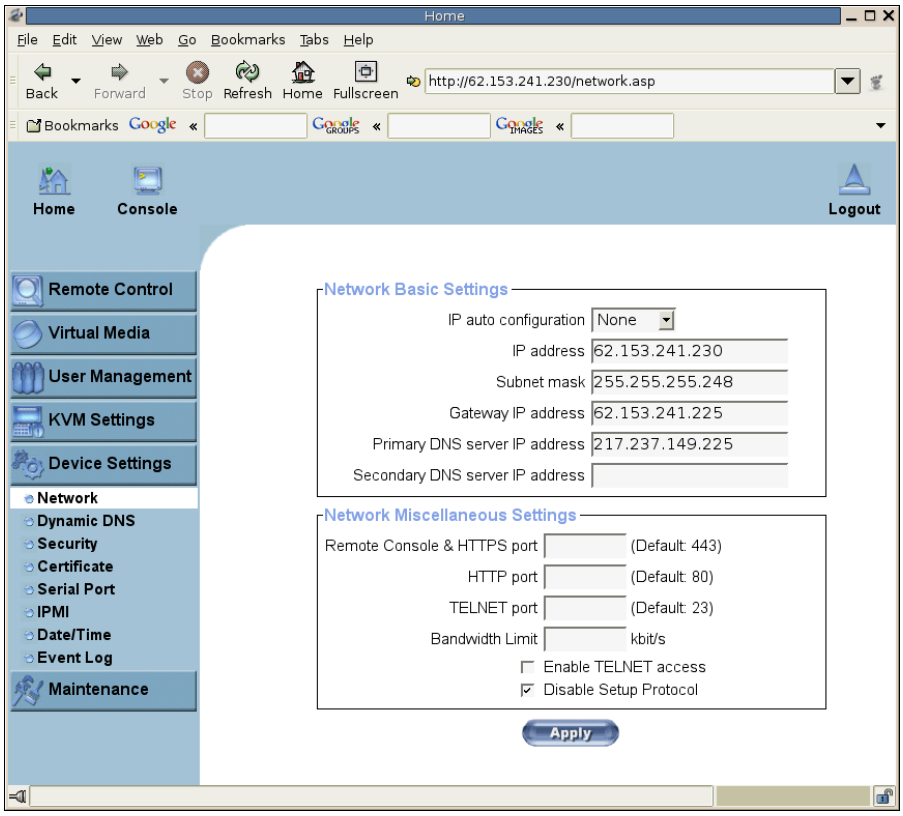

Figure 6-18. Network Settings

> **Warning**
>
> The initial IP configuration is usually done directly at the host system using the special procedure described in Table 4-1 .

> **Warning**
>
> Changing the network settings of the V-IP might result in losing connection to it. In case you change the settings remotely make sure that all the values are correct and you still have an option to access the V-IP .

Basic Network Settings

IP auto configuration

With this option you can define if the V-IP should fetch its network settings from a DHCP or BOOTP server. For DHCP select “ dhcp ” and for BOOTP select “ bootp ” accordingly. If you choose “ none ” then IP auto configuration is disabled.

IP address

IP address in the usual dot notation.

Subnet Mask

The net mask of the local network.

Gateway IP address

In case the V-IP should be accessible from networks other than the local one, this IP address must be set to the local network router's IP address.

Primary DNS Server IP Address

IP address of the primary Domain Name Server in dot notation. This option may be left empty, however the V-IP will not be able to perform name resolution.

Secondary DNS Server IP Address

IP address of the secondary Domain Name Server in dot notation. It will be used in case the Primary DNS Server cannot be contacted.

Miscellaneous Network Settings

Remote Console And HTTPS port

Port number at which the V-IP 's Remote Console server and HTTPS server are listening. If left empty the default value will be used.

HTTP port

Port number at which the V-IP 's HTTP server is listening. If left empty the default value will be used.

Telnet port

Port number at which the V-IP 's Telnet server is listening. If left empty the default value will be used.

Bandwidth Limit

The maximum network traffic generated through the V-IP Ethernet device. Value in Kbit/s.

Enable Telnet access

Set this option to allow accessing the V-IP using the Telnet gateway (see the Section called Telnet Console).

Disable Setup Protocol

Enable this option to exclude the V-IP from the setup protocol.

Dynamic DNS

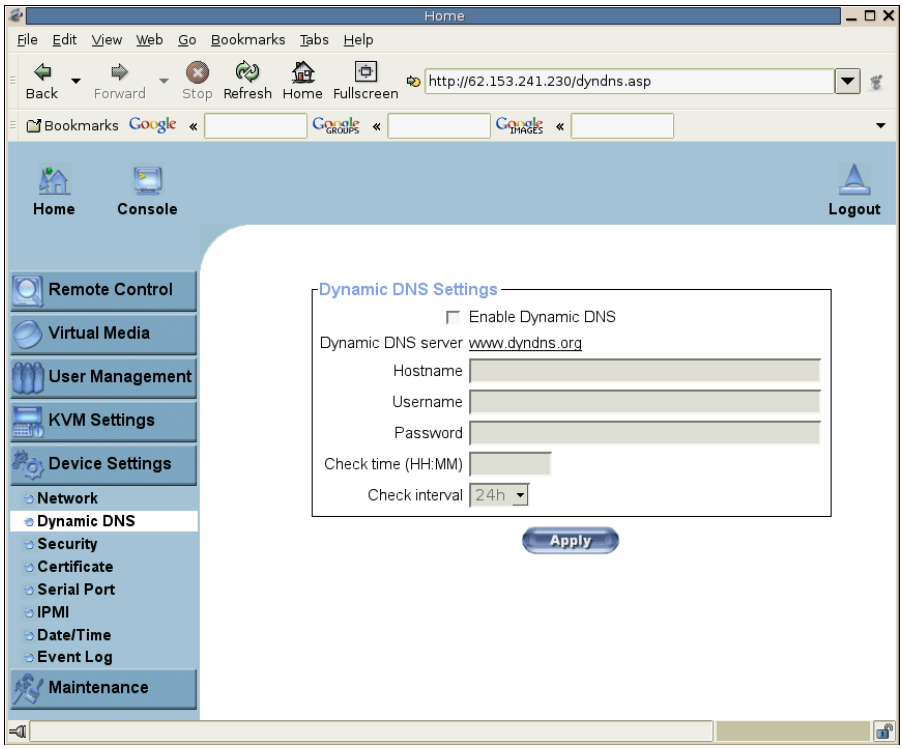

Figure 6-19. Dynamic DNS

A freely available Dynamic DNS service (`dyndns.org`) can be used in the following scenario (see Figure 6-20):

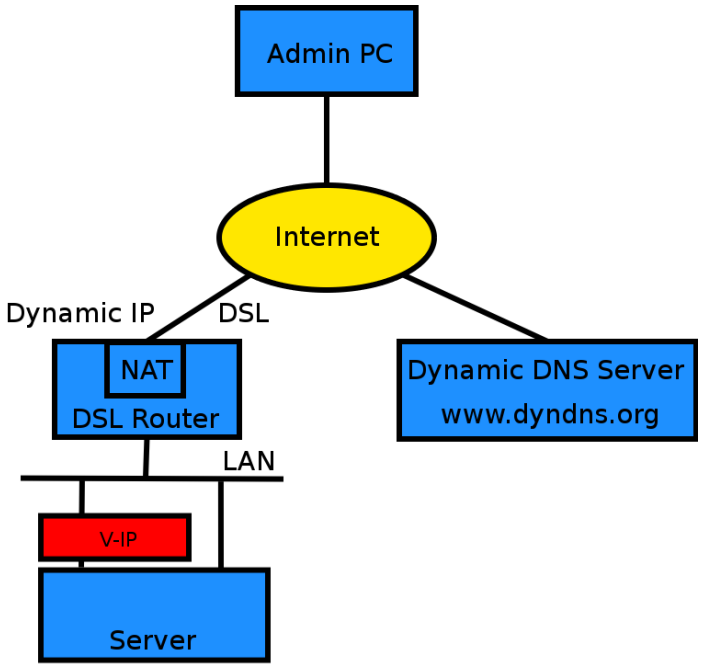

Figure 6-20. Dynamic DNS Scenario

The V-IP is reachable via the IP address of the DSL router which is dynamically assigned by the provider. Since the administrator does not know the IP address assigned by the provider, the V-IP connects to a special dynamic DNS server in regular intervals and registers its IP address there. The administrator may contact this server as well and pick up the same IP address belonging to his card. The administrator has to register a V-IP that is supposed to take part in the service with the Dynamic DNS Server and assign a certain hostname to it. He will get a nick- name and a password in return to the registration process. This account information together with the hostname is needed in order to determine the IP address of the registered V-IP . You have to perform the following steps in order to enable Dynamic DNS:

- Make sure that the LAN interface of the V-IP is properly configured.
- Enter the Dynamic DNS Settings configuration dialog as shown in Figure 6-19 .
- Enable Dynamic DNS and change the settings according to your needs (see below).

Enable Dynamic DNS
: This enables the Dynamic DNS service. This requires a configured DNS server IP address.

Dynamic DNS server
: This is the server name where V-IP registers itself in regular intervals. Currently this is a fixed setting since only `dyndns.org` is supported for now.

Hostname
: This is the hostname of the V-IP that is provided by the Dynamic DNS Server. (use the whole name including the domain, e.g. `testserver.dyndns.org` ,

not just the actual hostname).

Username

You have registered this username during your manual registration with the Dynamic DNS Server. Spaces are not allowed in the Nickname.

Password

You have used this password during your manual registration with the Dynamic DNS Server.

Check time

The V-IP card registers itself in the Dynamic DNS server at this time.

Check interval

This is the interval for reporting again to the Dynamic DNS server by the V-IP .

Warning

The V-IP has its own independent real time clock. Make sure the time setting of the V-IP is correct.

Security

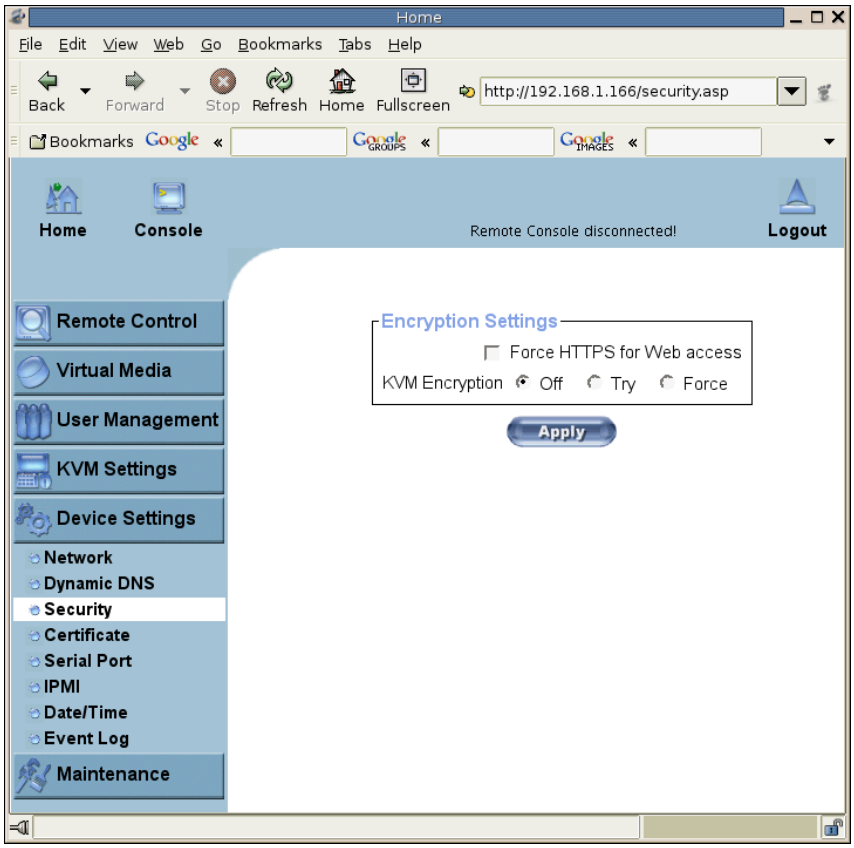

Figure 6-21. Device Security

Encryption Settings

Force HTTPS

If this option is enabled, access to the web front-end is only possible using a HTTPS connection. The V-IP will not listen on the HTTP port for incoming connections. In case you want to create your own SSL certificate that is used to identify the V-IP refer to the Section called Certificate .

KVM encryption

This option controls the encryption of the RFB protocol. RFB is used by the Remote Console to transmit both the screen data to the administrator machine and keyboard and mouse data back to the host. If set to “ Off ” no encryption will be used. If set to “ Try ” the applet tries to make an encrypted connection. In case that the connection cannot be established an unencrypted connection will be used instead. If set to “ Force ” the applet tries to make an encrypted connection. An error will be reported in case the connection establishment fails.

Certificate

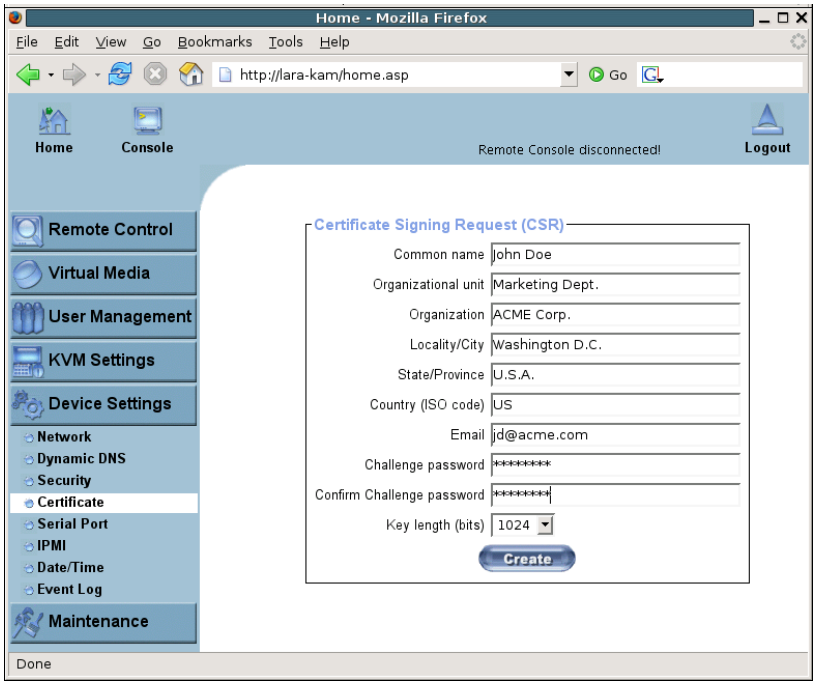

Figure 6-22. Certificate Settings

The V-IP uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment the V-IP has to expose its identity to a client using a cryptographic certificate. Upon delivery this certificate and the underlying secret key is the same for all V-IP ever produced and certainly will not match the network configuration that will be applied to the V-IP by its user. The certificate's underlying secret key is also used for securing the SSL handshake. Hence, this is a security risk (but far better than no encryption at all).
However, it is possible to generate and install a new base64 x.509 certificate that is unique for a particular V-IP . In order to do that, the V-IP is able to generate a new cryptographic key and the associated Certificate Signing Request (CSR) that needs to be certified by a certification authority (CA). A certification authority verifies that you are the person who you claim you are and signs and issues a SSL certificate to you.

To create and install a SSL certificate for the V-IP the following steps are necessary:

- Create a SSL Certificate Signing Request using the panel shown in Figure 6-22 . You need to fill out a number of fields that are explained below. Once this is done, click on the button " Create " which will initiate the Certificate Signing Request generation. The CSR can be downloaded to your administration machine with the " Download CSR " button (see Figure 6-23).
- Send the saved CSR to a CA for certification. You will get the new certificate from the CA after a more or less complicated traditional authentication process (depending on the CA).
- Upload the certificate to the V-IP using the " Upload " button as shown in Figure 6-23 .

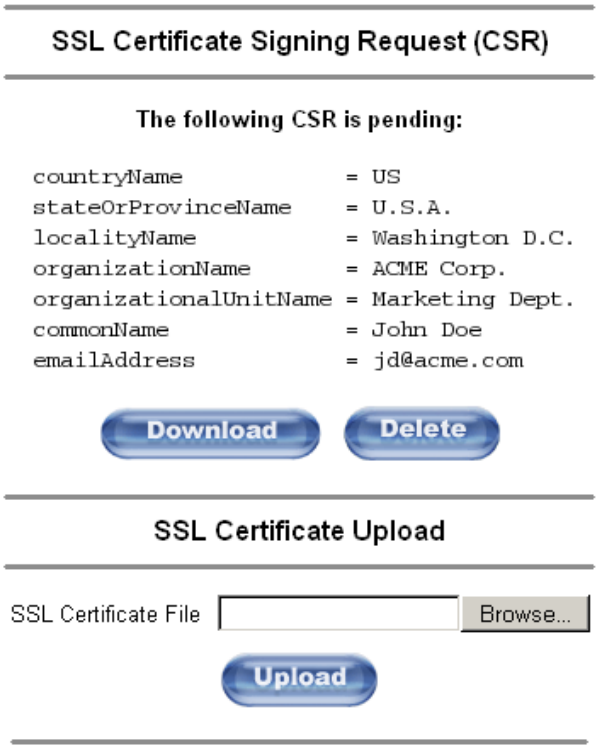

Figure 6-23. SSL Certificate Upload

After completing these three steps the V-IP has its own certificate that is used for identifying the card to its clients.

> **Warning**
>
> If you destroy the CSR on the V-IP there is no way to get it back! In case you deleted it by mistake, you have to repeat the three steps as described above.

Common name

This is the network name of the V-IP once it is installed in the user's network (usually the fully qualified domain name). It is identical to the name that is used to access the V-IP with a web browser but without the prefix " http:// " . In case the name given here and the actual network name differ, the browser will pop up a security warning when the V-IP is accessed using HTTPS.

Organizational unit

This field is used for specifying to which department within an organization the V-IP belongs.

Organization

The name of the organization to which the V-IP belongs.

Locality/City

The city where the organization is located.

State/Province

The state or province where the organization is located.

Country (ISO code)

The country where the organization is located. This is the two-letter ISO code, e.g. DE for Germany, or US for the U.S.

Challenge Password

Some certification authorities require a challenge password to authorize later changes on the certificate (e.g. revocation of the certificate). The minimal length of this password is four characters.

Confirm Challenge Password

Confirmation of the Challenge Password.

Email

The email address of a contact person that is responsible for the V-IP and its security.

Key length

This is the length of the generated key in bits. 1024 Bits are supposed to be sufficient for most cases. Longer keys may result in slower response time of the V-IP during connection establishment.

Serial Settings

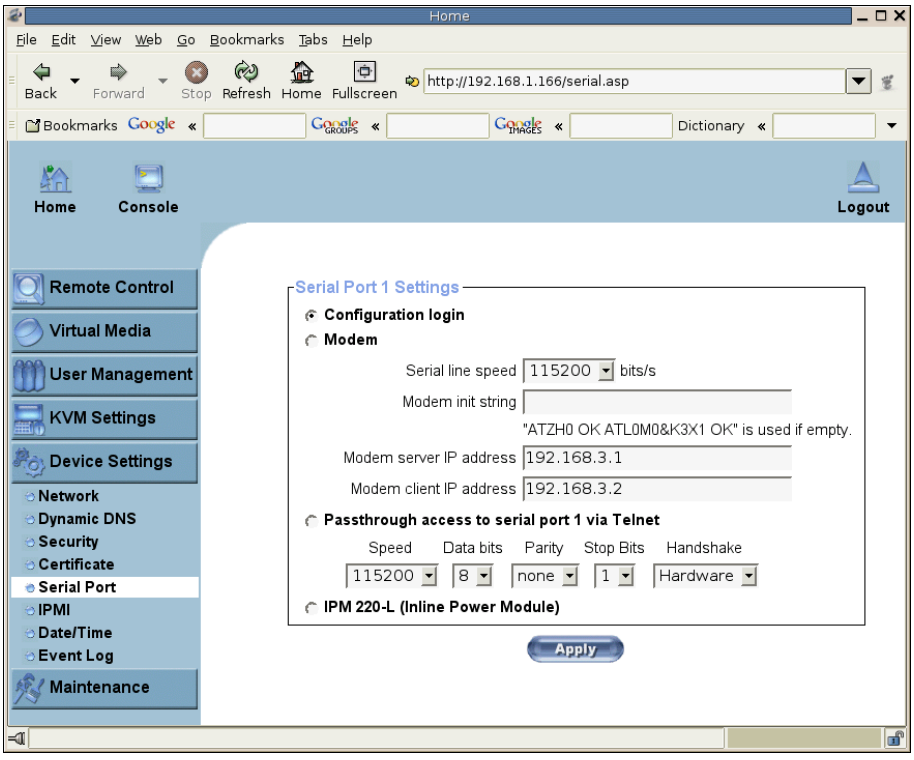

Figure 6-24. Serial Settings

The V-IP Serial Settings (Figure 6-24) allow you to specify what device is connected to the serial port and how to use it. To access the serial interface a port replicator cable is required .

Configuration or console login

Do not use the serial port for any special function, use it only for the initial configuration (see Table 4-1).

Modem

The V-IP offers remote access using a telephone line in addition to the standard access over the built-in Ethernet adapter. The modem needs to be connected to the serial interface of the V-IP .

Logically, connecting to the V-IP using a telephone line means nothing else than building up a dedicated point-to-point connection from your console computer to the V-IP . In other words, the V-IP acts as an Internet Service Provider (ISP) to which you can dial in. The connection is established using the Point-to-Point Protocol (PPP). Before you connect to the V-IP make sure to configure your console computer accordingly. For instance, on Windows based operating systems you can configure a dial-up network connection which defaults to the right settings like PPP. The Modem Settings panel allows you to configure the remote access to the V-IP using a modem. The meaning of each parameter will be described below. The modem settings are part of the serial settings panel .

Serial line speed

The speed with which the V-IP is communicating with the modem. Most of all modems available today will support the default value of 115.200 bps. In case you are using an old modem and discovering problems try to lower this speed.

Modem Init String

The initialization string used by the V-IP to initialize the modem. The default value will work with all modern standard modems directly connected to a telephone line. In case you have a special modem or the modem is connected to a local telephone switch that requires a special dial sequence in order to establish a connection to the public telephone network, you can change this setting by giving a new string. Refer to the modem's manual about the AT command syntax.

Modem server IP address

This IP address will be assigned to the V-IP itself during the PPP handshake. Since it is a point-to-point IP connection virtually every IP address is possible but you must make sure that it is not interfering with the IP settings of the V-IP and your console computer. The default value will work in most cases.

Modem client IP address

This IP address will be assigned to your console computer during the PPP handshake. Since it is a point-to-point IP connection virtually every IP address is possible but you must make sure that it is not interfering with the IP settings of the V-IP and your console computer. The default value will work in most cases.

Passthrough access to serial port via Telnet
: Using this option it is possible to connect an arbitrary device to the serial port and access it (assuming it provides terminal support) via Telnet. Select the appropriate options for the serial port and use the Telnet Console or a standard Telnet client to connect to the V-IP . For more information about the Telnet interface you may have a look at the Section called Telnet Console .

IPM 220-L (Inline Power Module)
: This is an optionally available external module to switch power of a single system by putting it in the power supply line of the controlled system.

Intelligent Platform Management Interface (IPMI)

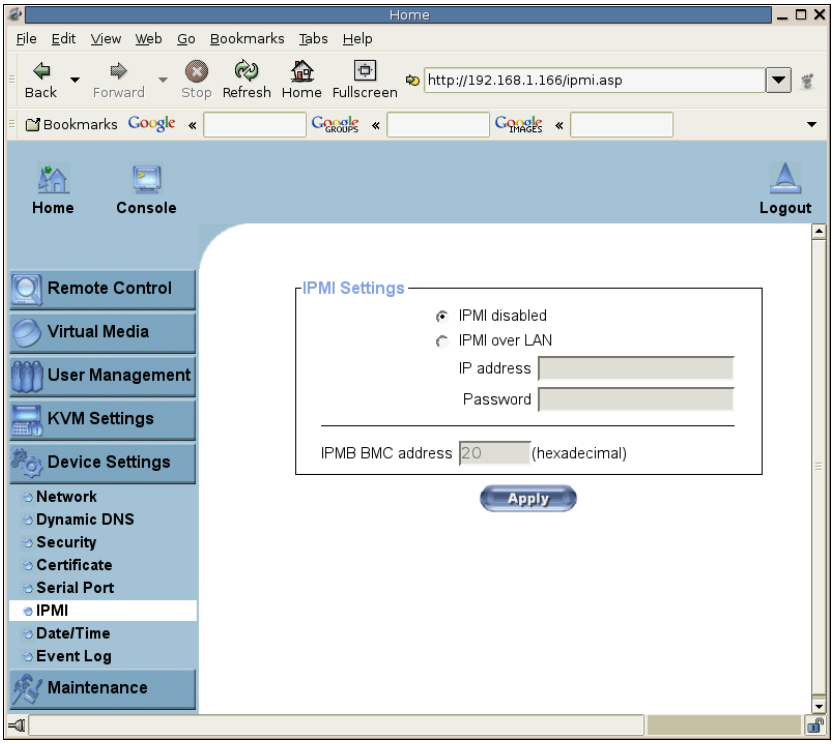

Figure 6-25. IPMI

Generals

By using the V-IP IPMI facilities you have an additional way to power on or off the system or to perform a hard reset. Furthermore, it provides the possibility to show an event log of the host system and the status of some system sensors (i.e. temperature). If your host system supports IPMI, you can access it by one of the following ways:

- IPMI over LAN (IPMI V1.5 is required)

IPMI Settings

Figure 6-25 shows the V-IP IPMI settings panel. Its options will be explained below.

IPMI disabled

Disables IPMI on the V-IP . This means that Status via IPMI and Event Log via IPMI are not available and the power on/off and reset functions do not use IPMI rather than the ATX and the reset cable connected from the V-IP to the mother-board.

IPMI over LAN

You can connect the IPMI over a LAN connection, too. The prerequisite for this access type is a host system with IPMI V1.5 and a network adapter with a side-band connection to the BMC (mostly on board). In the IPMI Settings you have to enter the IP address of this host system and the correct password for the LAN connection. You can also access other IPMI systems if you enter their IP address.

Date And Time

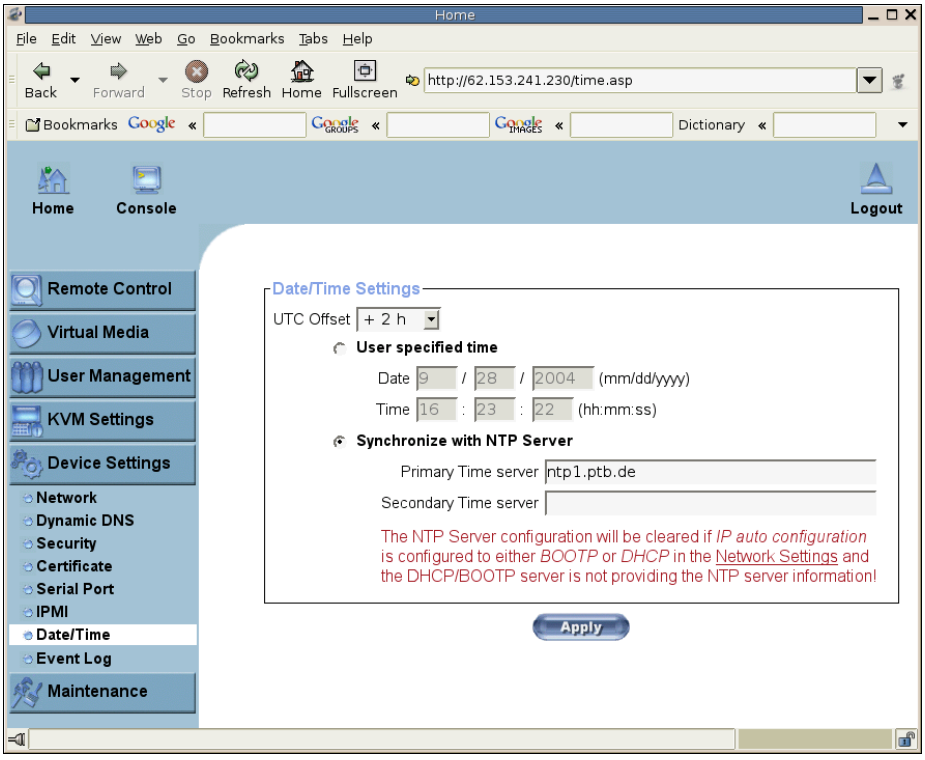

Figure 6-26. Date and Time

This link refers to a page where the internal realtime clock of the V-IP can be set up (see Figure 6-26). You have the possibility to adjust the clock manually or to use a NTP time server. Without a time server your time setting will not be persistent, so you have to adjust it again after the V-IP loses power for more than a few minutes. To avoid this you can use a NTP time server which sets up the internal clock auto-

matically to the current UTC time. Because NTP server time is always UTC, there is a setting that allows you to set up a static offset to get your local time.

> **Warning**
>
> There is currently no way to adjust the daylight saving time automatically. So you have to set up the UTC offset twice a year properly to the local rules of your country.

Event Log

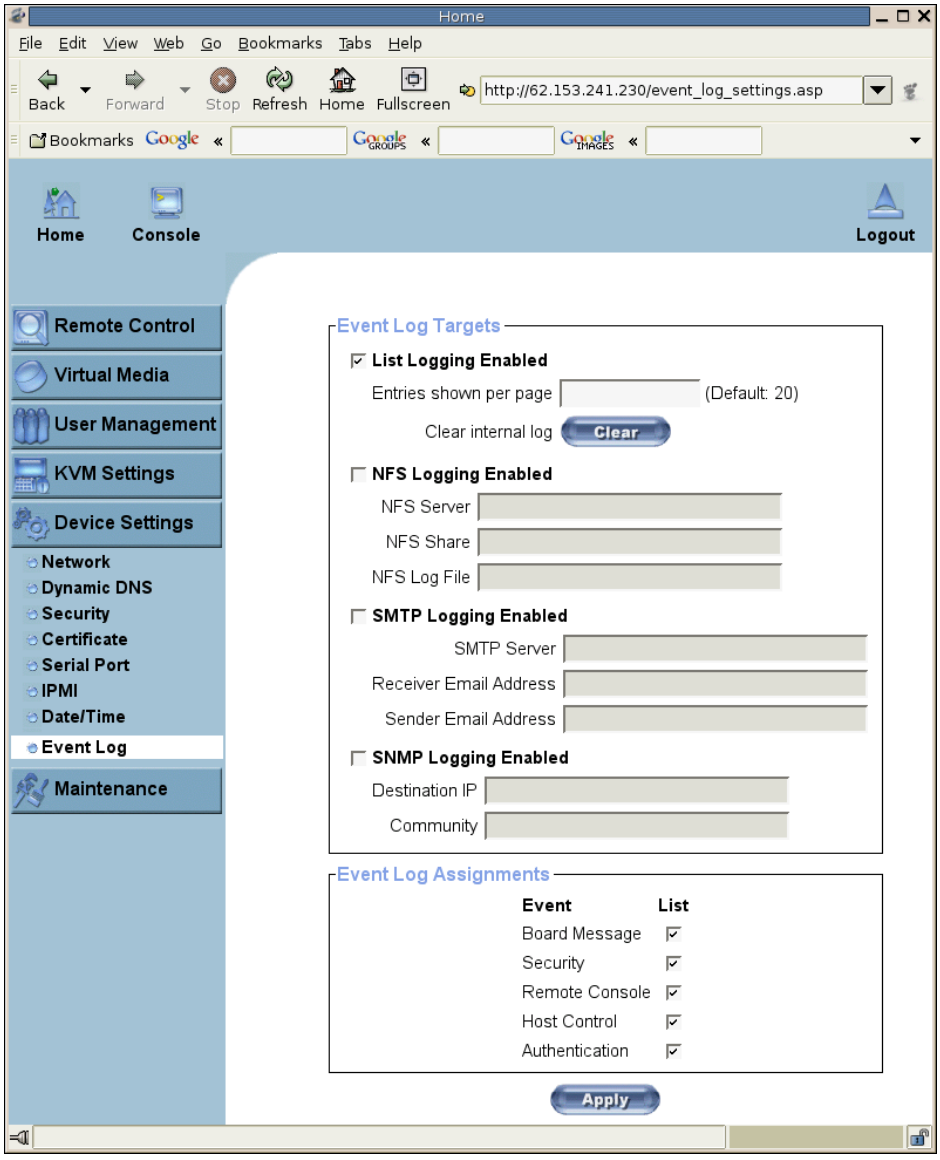

Figure 6-27. Event Log

Important events like a login failure or a firmware update are logged to a selection of logging destinations (see Figure 6-27). Each of those events belong to an event group which can be activated separately.
The common way to log events is to use the internal log list of the V-IP . To show the log list click on " Event Log " on the " Maintenance " page. In the Event Log Settings you can choose how many log entries are shown on each page. Furthermore, you can clear the log file here.

Event Log Targets

List logging enabled

To log events you may use the internal log list of the V-IP . To show the log list click on " Event Log " on the " Maintenance " page.

Since the V-IP 's system memory is used to save all the information, the maximum number of possible log list entries is restricted to 1.000 events. Every entry that exceeds this limit overrides the oldest one automatically.

Warning

If the reset button on the HTML frontend is used to restart the V-IP , all logging information is saved permanently and is available after the V-IP has been started. If the V-IP loses power or a hard reset is performed, all logging data will be lost. To avoid this use one of the log methods described below.

NFS Logging enabled

Define a NFS server where a directory or a static link has to be exported to, in order to write all logging data to a file that is located there. To write logging data from more than one V-IP devices to only one NFS share, you have to define a file name that is unique for each device. When you change the NFS settings and press the button " Apply " , the NFS share will be mounted immediately. That means the NFS share and the NFS server must be filled with valid sources or you will get an error message.

Warning

In contrast to the internal log file on the V-IP , the size of the NFS log file is not limited. Every log event will be appended to the end of the file so it grows continuously and you may have to delete it or move it away from time to time.

SMTP Logging enabled

With this option the V-IP is able to send Emails to an address given by the Email address text field in the Event Log Settings. These mails contain the same description strings as the internal log file and the mail subject is filled with the event group of the occurred log event. In order to use this log destination you have to specify a SMTP server that has to be reachable from the V-IP device and that needs no authentication at all (<serverip>:<port>).

SNMP Logging enabled

If this is activated, the V-IP sends a SNMP trap to a specified destination IP address, every time a log event occurs. If the receiver requires a community string,

you can set it in the appropriate text field. Most of the event traps only contain one descriptive string with all information about the log event. Only authentication and host power events have an own trap class that consists of several fields with detailed information about the occurred event. To receive this SNMP traps any SNMP trap listener may be used.

Event Log Assignments

You may choose which actions of the V-IP will be saved in the log file. Tick the desired box(es) and click “ Apply ” to confirm your selection.

Maintenance

Device Information

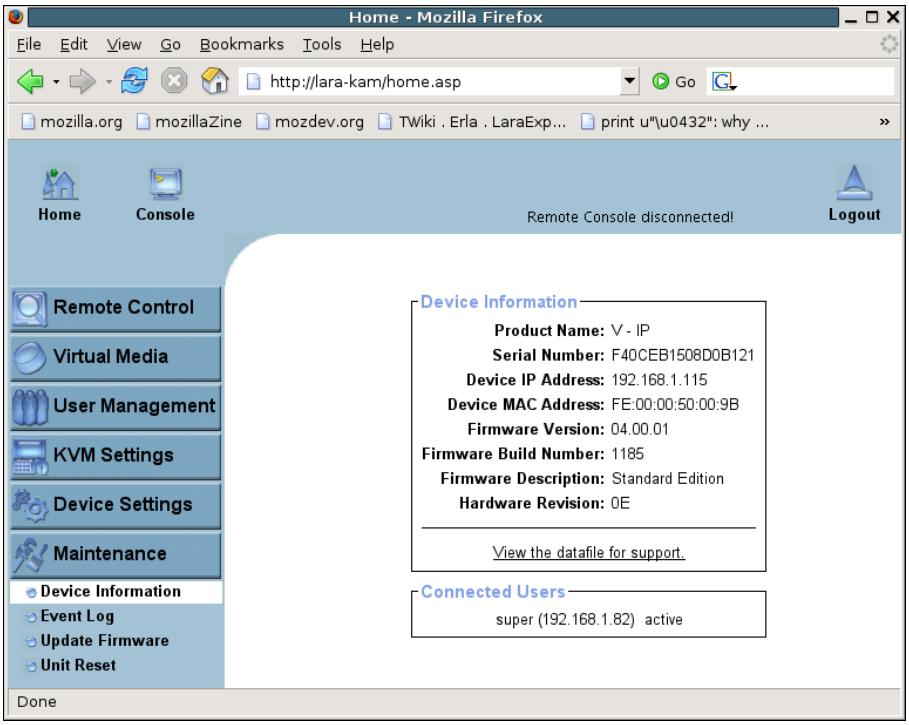

Figure 6-28. Device Information

This section contains a summary with various information about this V-IP and its current firmware and allows you to reset the card. You may have a look at Figure 6-28 for an example.

The Data file for support allows you to download the V-IP data file with specific support information. This is an XML file with certain customized support information like the serial number etc. You may send us this information together with a support request. It will help us to locate and solve your reported problem.

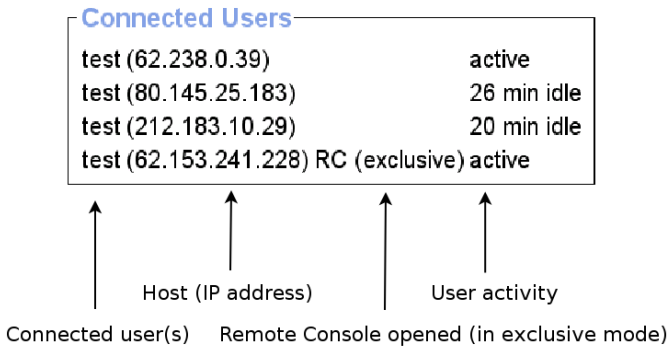

Figure 6-29. Connected Users

Figure 6-29 displays the V-IP activity. From left to right the connected user(s), its IP address (from which host the user comes from) and its activity status is displayed. “ RC ” means that the Remote Console is open. If the Remote Console is opened in “ exclusive mode ” the term “ (exclusive mode) ” is added. For more information about this option see the Section called Remote Console Control Bar in Chapter 5 . To display the user activity the last column contains either the term “ active ” for an active user or “ 20 min idle ” for a user who is inactive for a certain amount of time.

Event Log

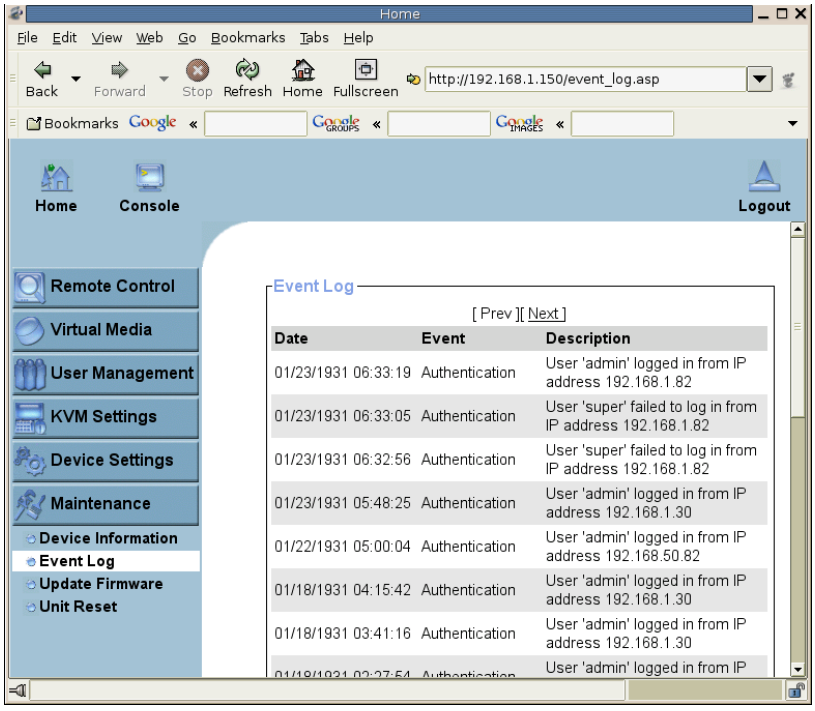

Figure 6-30. Event Log List

Figure 6-30 displays the Event Log list. It includes the events that are kept by the V-IP extended by the event date, a short event description and an IP address the request was sent from. You may use the text buttons “ Prev ” and “ Next ” to browse within the data.

Update Firmware

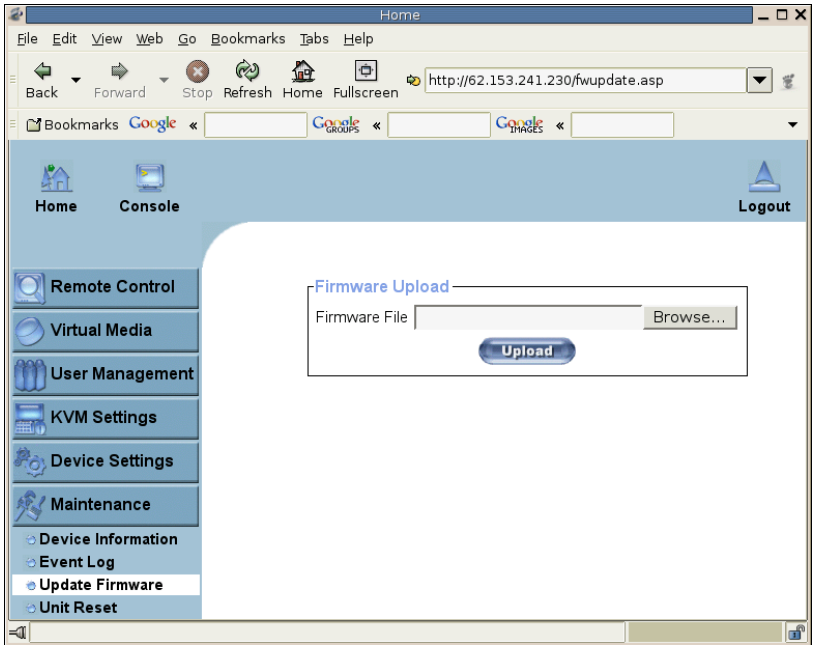

Figure 6-31. Update Firmware

The V-IP is a complete standalone computer. The software it runs is called the firmware. The firmware of the V-IP can be updated remotely in order to install new functionality or special features.
A new firmware update is a binary file which will be sent to you by email or which you can download from the HETEC web site. If the firmware file is compressed (file suffix `.zip`) then you have to unzip it before you can proceed. Under the Windows operating system you may use WinZip from `http://www.winzip.com/` for decompression. Other operating systems might already provide a program that is called `unzip` .

Before you can start updating the firmware of your V-IP the new uncompressed firmware file has to be accessible on the system that you use for connecting to the V-IP .

Updating the firmware is a three-stage process:

- Firstly, the new firmware file is uploaded onto the V-IP . In order to do that you need to select the file on your local system using the button “ Browse ” of the Upload Firmware panel (see Figure 6-31). Then, click “ Upload ” to transfer the previously selected file from your local file system onto the V-IP . Once the firmware file has been uploaded, it is checked whether it is a valid firmware file and whether

 there were any transmission errors. In case of any error the Upload Firmware func- tion will be aborted and the current firmware is kept as is.

- Secondly, if everything went well, you see the Update Firmware panel . The panel shows you the version number of the currently running firmware and the version number of the uploaded firmware. Pressing the button “ Update ” will store the new version and substitute the old one completely.

> **Warning**
>
> This process is not reversible and might take some minutes. Make sure the V-IP ’s power supply will not be interrupted during the update process, because this may cause an unusable device.

- Thirdly, after the firmware has been stored, the V-IP will reset automatically. After about one minute you will be redirected to the Login page and requested to login once again.

> **Warning**
>
> The three-stage firmware update process and complete consistency check are making a mistake in updating the firmware almost impossi- ble. However, only experienced staff members or administrators should perform a firmware update. Make sure the V-IP ’s power supply will not be interrupted!

Unit Reset

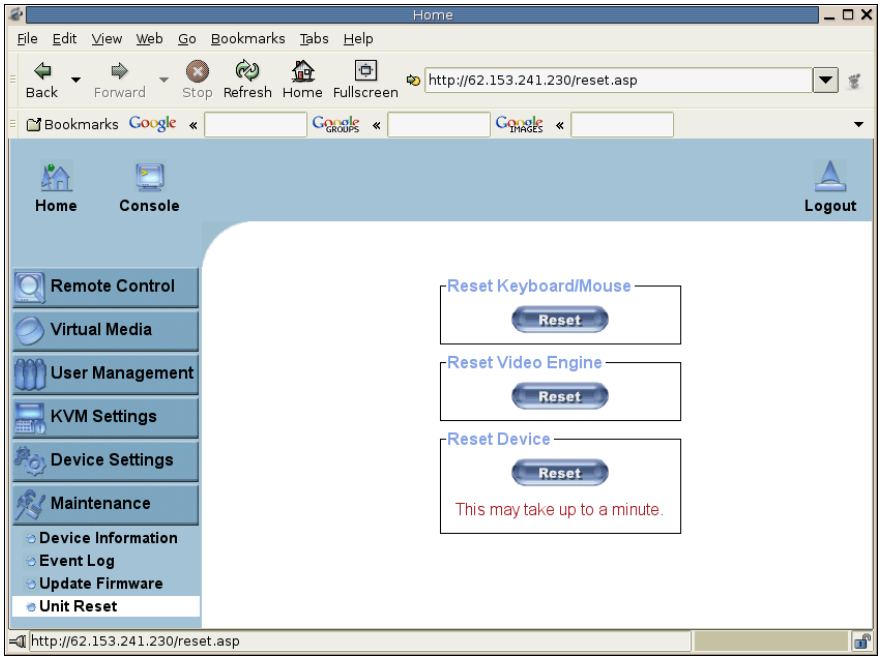

Figure 6-32. Unit Reset

This section allows you to reset specific parts of the device. This involves the both keyboard and mouse, the video engine and the V-IP itself. Resetting the card itself is mainly needed to activate a newly updated firmware. It will close all current connections to the administration console and to the Remote Console. The whole process will take about half a minute. Resetting subdevices (e.g. video engine) will take some seconds only and does not result in closing connections.

To reset a certain V-IP functionality click on the button “ Reset ” as displayed in Figure 6-32 .

Note: Only the superuser is allowed to reset the V-IP .

Appendix A. Frequently Asked Questions

1. The remote mouse does not work or is not synchronous. First, check the VGA connection. Both the V-IP and the local monitor have to support the same video resolution. Make sure that your mouse settings match your mouse model, i.e. PS/2 or wheel mouse. The mouse model has to be set similarly on both the V-IP and the Operating System you use on your host. In some circumstances the mouse synchronization process could behave incorrectly, refer to the Section called Mouse, Keyboard and Video configuration in Chapter 4 for further explanation.

2. The video quality is bad or the picture is grainy. Use the Remote Console menu entry " Reset " to set the V-IP to its default values. Then, press the Auto Adjust button to select an appropriate video output.

3. Login on the V-IP fails. Verify both your user login and your password. On default, the user " admin " has the password " hetec " . Moreover, your web browser has to be configured to accept cookies.

4. The Remote Console window of the V-IP does not open. A firewall may prevent the access to the Remote Console. The TCP ports #80 (for HTTP) and #443 (for both HTTPS and RFB) have to be open (the server providing the firewall has to accept incoming TCP connections on these ports).

5. Remote console is unable to connect and displays a timeout error. Have a look on your hardware. If there is a proxy server between the V-IP and your host, then you may not be able to transfer the video data using RFB. Establish a direct connection between the V-IP and the client.

Furthermore, check the settings of the V-IP and choose a different server port used for RFB transfer. If you use a firewall then check the according port for accepting connections. You may restrict these connections for the IP addresses used by the V-IP and your client.

6. No connection can be established to the V-IP . Have a look on your hardware. Is the V-IP attached to a power supply? Verify your network configuration (IP address, router). You may send a " ping " request to the V-IP to find out whether the V-IP is reachable via network.

7. Special key combinations, e.g. ALT+F2, ALT+F3 are intercepted by the console system and not transmitted to the host.

You have to define a so-called " Button Key " . This can be done in the Remote Console settings (see the Section called Remote Console Control Bar in Chapter 5).

8. The V-IP web pages are not displayed correctly. Check your browser's cache settings. Make sure the cache settings are not set to something like " never check for newer pages " . Otherwise the V-IP pages may be loaded from your browser cache and not from the card.

9. Windows XP does not awake from standby mode. This is possibly a Windows XP problem. Try not to move the mouse pointer while XP switches into standby mode.

10. For SUN computers a USB keyboard does not work.

The V-IP emulates a USB keyboard. If you attach a USB keyboard to your host two keyboards are detected. It cannot be predicted which one of these comes first and you will be able to work with. SUN supports only one USB keyboard.

11. Cannot upload the signed certificate in MacOS X. If an " internal error " occurs while uploading the signed certificate either change the extension of the file to `.txt` or add a file helper using the Internet Explorer preferences for this type of file. Make sure that the encoding is set to " plain text " and the checkbox " use for outgoing " is set. As an alternative, you may also use a Mozilla based browser (Mozilla, FireFox).

12. Every time I open a dialog box with some buttons the mouse pointers are not synchronous anymore. Disable the setting " Automatically move mouse pointer to the default button of dia- log boxes " in the mouse settings of your operating system.

13. The Remote Console does not open with Opera in Linux. Some versions of Opera do not grant enough permissions if the signature of the ap- plet cannot be verified. To solve the problem, add the lines

```
grant codeBase "nn.pp.rc.RemoteConsoleApplet" {
   permission java.lang.RuntimePermission
   "accessClassInPackage.sun.*";
```

to the java policy file of opera (e.g. `/usr/share/opera/java/opera.policy`).

14. The Remote Console remains black.

Check the V-IP for being USB powered only. If there is not enough power via USB the remote Console opens but remain black. Attach an external power supply to the V-IP . Verify the V-IP settings using the according section in the front end.

15. The video data on the local monitor is surrounded by a black border. This is not a failure. The local monitor is programmed to a fixed video mode that can be selected in the video settings of the V-IP . Refer to the Section called Remote Console Control Bar in Chapter 5 for further planation.

16. I forgot my password. How can I reset the V-IP to factory defaults? You may use the serial interface . For a detailed description see the Section called Resetting the V-IP to its Factory Settings in Chapter 4 .

Appendix B. Glossary

ACPI Advanced Configuration and Power

Interface

A specification that enables the operating system to implement power management and system configuration.

ATX

Advanced Technology Extended A particular specification that covers the style of motherboards and enclosure introduced by Intel in 1995.

DHCP Dynamic Host Configuration

Protocol

A protocol for dynamically assigning IP configurations to host names, especially used in a local network.

DNS Domain Name

System

A protocol used to locate computers on the Internet by their name.

FAQ Frequently Asked

Questions

HTTP Hypertext Transfer

Protocol

One of the protocols used for communication between single computers, especially between web browsers and web servers.

HTTPS Hypertext Transfer Protocol

Secure The secure version of HTTP.

LED

Light Emitting Diode A semiconductor device that emits incoherent monochromatic light when elec- trically biased in the forward direction.

PS/2

Personal System/2

IBM's second generation of personal computers, which was released to the public in 1987. Today, PS/2 is known as a device interface for mouse and keyboard.

SNMP Simple Network Management

Protocol

A widely used network monitoring and control protocol.

SSL

Secure Socket Layer

 An encryption technology for the Internet used to provide secured data trans- missions.

SVGA Super Video Graphics

Array

A refinement of the Video Graphics Array (VGA) that provides increased pitch and resolution performance.

UTP

Unshielded Twisted Pair A cable with two conductors twisted as a pair and bundled within the same outer PVC covering.

Appendix C. V-IP Video Modes

Table C-1 lists the video modes the V-IP supports. Please do not use any other custom video settings besides of these. If done so, the V-IP may not be able to detect them.

Table C-1. V-IP Video Modes

Resolution (x,y)	Refresh Rates (Hz)
640x340	70, 85
640x400	56, 85
640x480	60, 67, 72, 75, 85, 90, 100, 120
720x400	70, 85
800x600	56, 60, 70, 72, 75, 85, 90, 100
832x624	75
1024x768	60, 70, 72, 75, 85, 90, 100
1152x864	75
1152x870	75
1152x900	66, 76
1280x960	60, 85
1280x1024	60, 75, 85
1600x1200	60, 65, 70, 75
2048x1536	85 (local port only)

Appendix D. Users and Roles

Table D-1. Roles

Frontend Section	Regular User	Administrator	Superuser
Remote Control: KVM	x	x	x
Remote Control: Remote Power	-	x	x
Remote Control: Telnet Console	x	x	x
Virtual Media	x	x	x
User Management: Change Password	x	x	x
User Management: Users	-	-	x
KVM Settings: User Console	x (w/o Misc. Settings)		
KVM Settings: Keyboard/Mouse	-	x	x
KVM Settings: Video	-	x	x
Device Settings	-	-	x
Maintenance: Device Information	x	x	x
Maintenance: Event Log	-	-	x
Maintenance: Update Firmware	-	-	x
Maintenance: Unit Reset	Keyboard/ Mouse, Video	Keyboard/ Mouse, Video	Keyboard/ Mouse, Video, Device

Appendix E. Key Codes

Table E-1 shows the key codes used to define the key strokes or hotkeys for several functions. Please note that these key codes do not necessarily represent the key characters that are used on international keyboards. A key on a standard 104 key PC keyboard with a US English language mapping is named. The layout for this keyboard is shown in Figure E-1 . However, most modifier keys and other alphanumeric keys used for hotkey purposes in application programs are on a similar position, no matter what language mapping you are using. Some of the keys also have aliases. This means that a key can be named by two different key codes.

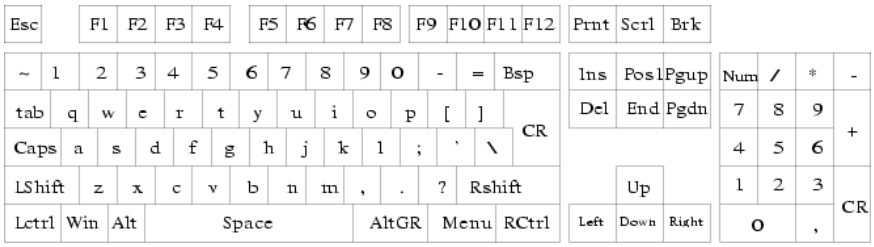

Figure E-1. English (US) keyboard Layout, used for the key codes

Table E-1. Key Names

Key	Alias Key(s)
0 - 9	
A - Z	
~	TILDE
_	MINUS
=	EQUALS
;	
'	
<	LESS
,	
.	
/	SLASH
BACKSPACE	
TAB	
[	
]	
ENTER	
CAPS LOCK	
\	BACK SLASH
LSHIFT	SHIFT RCTRL
CTRL, STRG RSHIFT	
SHIFT LCTRL	CTRL,
STRG	

Key	Alias Key(s)
LALT	ALT
SPACE	
ALT GR ESCAPE	
ESC F1	
F2	
F3	
F4	
F5	
F6	
F7	
F8	
F9	
F10	
F11	
F12	
PRINTSCREEN	
SCROLL LOCK	
BREAK	
INSERT HOME	
POS 1	
PAGE_UP	
PAGE_DOWN	
DELETE	DEL
END	
UP	
LEFT	
DOWN	
RIGHT	
NUM_LOCK	
NUMPAD0	
NUMPAD1	
NUMPAD2	
NUMPAD3	
NUMPAD4	
NUMPAD5	
NUMPAD6	
NUMPAD7	
NUMPAD8	
NUMPAD9	
NUMPADPLUS	NUMPAD_PLUS, +

Key	Alias Key(s)
NUMPAD /	/ NUMPADMUL
NUMPAD_MUL, x	NUMPADMINUS
NUMPAD_MINUS, -	
NUMPADENTER	
WINDOWS	
MENU	

Appendix F. Pin Assignment

VGA HD-15

Figure F-1. VGA HD-15

Table F-1. VGA HD-15

Pin	Assignment	Pin	Assignment
1	Red	9	USB+5V
2	Green	10	GND sync
3	Blue	11	USB_D+
4	USB_D -	12	SDA, DDC ...
5	GND	13	HSYNC
6	GND red	14	VSYNC
7	GND green	15	SCL, DDC
8	GND blue		

RJ45 Connector Ethernet

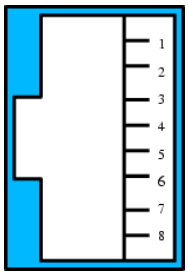

Figure F-2. RJ45

Table F-2. RJ45

Pin	Assignment	Pin	Assignment
1	TX +	5	Not connected
2	TX -	6	RX-
3	RX +	7	Not connected
4	Not connected	8	Not connected

Appendix G. Specifications

Sizes and Weight

Table G-1. V-IP Specification

Attribute	Value
Height	
Width	
Length	
Weight	
Housing	
Power Consumption	

Environment

Temperature

Table G-2. Temperature

Attribute	Value
Operating	0 C to 40 C (32 F to 131 F)
Storage	-18 C to 70 C (-20 F to 158 F)

Humidity

Table G-3. Humidity

Attribute	Value
Operating	10% to 90% (non-condensing)
Storage	5% to 95% (non-condensing)

Appendix H. V-IP Operation Advices

This device has to be operated with the provided power supply only (HETEC SA-051A5F-12). The use of other power supplies voids the product liability of the manufacturer. If the power supply shows a malfunction, it must not be opened. Instead a request a replacement from the manufacturer or the vendor. The power cord of the power supply is the point of junction to the supply network AC 230 V. Therefore both the power supply and the socket have to be easily accessible to disconnect them quickly if it is necessary.

Appendix I. HETEC Warranty Information

Limited Warranty HETEC Datensysteme GmbH, Germering, Germany (“ HETEC ”) manufactures its hardware products from parts and components that are new or equivalent to new in accordance with industry-standard practices. HETEC warrants that the hardware products including the firmware will be free from defects in materials and work- manship under normal use. Any implied warranties on the HETEC firmware and hardware are limited to 24 months, respectively, beginning on the date of invoice. Some states/jurisdictions do not allow limitations on duration of an implied war- ranty, so the above limitation may not apply to you. Additionally HETEC grants a special warranty for 6 month.

Customer Remedies HETEC ’s entire liability and exclusive remedy shall be, at HETEC ’s option, either (a) return of the price paid, or (b) repair or replacement of the firmware or hardware that does not meet this Limited Warranty and which is returned to HETEC with a copy of your receipt. Damage due to shipping the products to you is covered under this warranty. Otherwise warranty does not cover damage due to external causes, includ- ing accident, abuse, misuse, problems with electrical power, servicing not authorized by HETEC , usage not in accordance with product instructions, failure to perform required preventive maintenance and problems caused by use of parts and compo- nents not supplied by HETEC . Any replacement hardware will be warranted for the remainder of the original period or thirty (30) days, whichever is longer. HETEC will repair or replace products returned to HETEC ’s facility. To request warranty service you must inform HETEC within the warranty period. If warranty service is required, HETEC will issue a Return Material Authorization Number. You must ship the prod- ucts back to HETEC in their original or an equivalent packaging, prepay shipping charges, and insure the shipment or accept the possibility of loss or damage during shipment.

No Other Warranties To the maximum extend permitted by applicable law, HETEC disclaim all other war- ranties, either express or implied, including, but not limited to implied warranties of merchantability and fitness for a particular purpose, with regard to the firmware, the accompanying written materials, and any accompanying hardware. This lim- ited warranty gives you specific legal rights. You may have others, which vary from state/jurisdiction to state/jurisdiction.

No Liability For Consequential Damages To the maximum extent permitted by applicable law, in no event shall HETEC be liable for any damages whatsoever (including without limitation, special, incidental, consequential or indirect damages for personal injury, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this prod- uct, even if HETEC has been advised of the possibility of such damages. In any case, HETEC ’s entire liability under any provision of this agreement shall be limited to the amount actually paid by you for the firmware and/or hardware. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequen- tial or incidental damages, the above limitation may not apply to you.

Appendix I. HETEC Warranty Information